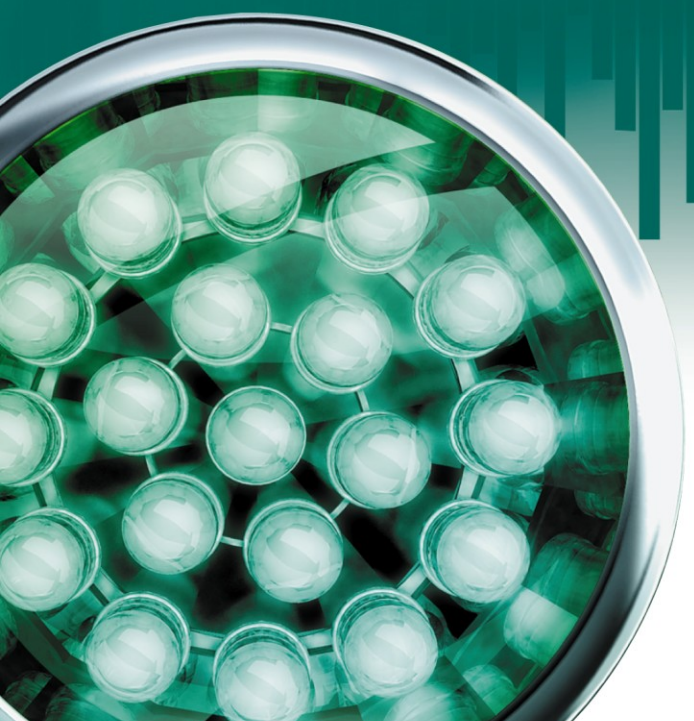
Kaspersky Anti-Virus 2011

MANUAL DO USUÁRIO

VERSÃO DO APLICATIVO: 11.0 CF1



KASPERSKY lab

Prezado usuário,

Obrigado por escolher nosso produto. Esperamos que este documento seja útil para você e responda à maioria das dúvidas que possam aparecer.

Aviso! Este documento é propriedade da Kaspersky Lab ZAO (também chamada de Kaspersky Lab): todos os seus direitos são reservados pelas leis de direitos autorais da Federação Russa e por tratados internacionais. A reprodução e distribuição ilegais deste documento ou de partes dele resultarão em responsabilidades civis, administrativas ou criminais relativas de acordo com a legislação aplicável.

Qualquer tipo de reprodução ou distribuição de qualquer material, incluindo sua tradução, é permitido somente através da permissão por escrito da Kaspersky Lab.

Este documento e as imagens gráficas relacionadas podem ser usados exclusivamente para fins informativos, não comerciais ou pessoais.

Este documento pode ser alterado sem qualquer notificação. A versão mais recente deste documento está disponível no site da Kaspersky Lab, em http://www.kaspersky.com/docs.

A Kaspersky Lab não assume qualquer responsabilidade pelo conteúdo, qualidade, relevância ou precisão do material usado neste documento cujos direitos são de propriedade de terceiros, ou por possíveis danos associados ao uso desses documentos.

Este documento contém marcas registradas e marcas de serviço que são propriedade de seus respectivos proprietários.

Data de revisão do documento: 24/6/2010

© 1997-2010 Kaspersky Lab ZAO. Todos os direitos reservados.

http://brazil.kaspersky.com/
http://brazil.kaspersky.com/suporte/

CONTEÚDO

CONTRATO DE LICENÇA DO USUÁRIO FINAL DA KASPERSKY LAB 9

SOBRE ESTE MANUAL 18

Nesta documentação 18

Convenções da documentação 20

FONTES ADICIONAIS DE INFORMAÇÕES 21

Fontes de informações para pesquisas independentes 21

Discutindo os aplicativos da Kaspersky no fórum da Web 22

Entrando em contato com o Departamento de vendas 22

Entrando em contato com o grupo de desenvolvimento da Documentação 22

KASPERSKY ANTI-VIRUS 2011 23

Novidades 23

Assegurando a proteção do computador 23

Kit de distribuição 25

Serviços para usuários registrados 25

Requisitos de hardware e software 26

INSTALANDO E REMOVENDO O APLICATIVO 27

Procedimento de instalação padrão 27

Etapa 1. Localizando a versão mais recente do aplicativo 28

Etapa 2. Verificando se o sistema atende aos requisitos de instalação 28

Etapa 3. Selecionar o tipo de instalação 29

Etapa 4. Examinando o contrato de licença 29

Etapa 5. Declaração sobre coleta de dados do Kaspersky Security Network 29

Etapa 6. Procurando aplicativos incompatíveis 29

Etapa 7. Selecionando a pasta de destino 30

Etapa 8. Preparando a instalação 30

Etapa 9. Instalando 31

Etapa 10. Ativando o aplicativo 31

Etapa 11. Registrando um usuário 31

Etapa 12. Concluindo a ativação 32

Etapa 13. Conclusão do Assistente 32

Atualizando a versão anterior do Kaspersky Anti-Virus 32

Etapa 1. Localizando a versão mais recente do aplicativo 33

Etapa 2. Verificando se o sistema atende aos requisitos de instalação 33

Etapa 3. Selecionar o tipo de instalação 34

Etapa 4. Examinando o contrato de licença 34

Etapa 5. Declaração sobre coleta de dados do Kaspersky Security Network 34

Etapa 6. Procurando aplicativos incompatíveis 34

Etapa 7. Selecionando a pasta de destino 35

Etapa 8. Preparando a instalação 35

Etapa 9. Instalando 36

Etapa 10. Concluindo a ativação 36

Etapa 11. Conclusão do Assistente 36

Cenários de instalação diferentes do padrão 36

Iniciando 37

Removendo o aplicativo 37
Etapa 1. Salvando dados para usar novamente 37
Etapa 2. Confirmação da remoção do aplicativo....38
Etapa 3. Removendo o aplicativo Concluindo a remoção....38
GERENCIANDO A LICENÇA....39
Sobre o Contrato de Licença do Usuário Final 39
Sobre a licença....39
Sobre o código de ativação 40
Exibindo informações da licença 40
INTERFACE DO APLICATIVO 42
Ícone da área de notificação....42
Menu de contexto 43
Janela principal do Kaspersky Anti-Virus....44
Janelas de notificação e mensagens pop-up....46
Janela de configuração do aplicativo....48
Kaspersky Gadget 49
INICIANDO E INTERROMPENDO O APLICATIVO....50
Ativando e desativando a execução automática....50
Iniciando e interrompendo o aplicativo manualmente....50
STATUS DE PROTEÇÃO DO COMPUTADOR....51
Diagnóstico e eliminação de problemas na proteção do computador 51
Ativando e desativando a proteção 53
Pausando e reiniciando a proteção 54
SOLUCIONANDO TAREFAS TÍPICAS....55
Como ativar o aplicativo 55
Como comprar ou renovar a licença....56
O que fazer quando forem exibidas notificações do aplicativo 57
Como atualizar os bancos de dados e módulos do aplicativo 57
Como verificar as áreas críticas do computador quanto à presença de vírus 58
Como verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus....59
Como executar a verificação completa do computador quanto à presença de vírus....60
Verificando vulnerabilidades no computador....61
Como proteger seus dados pessoais contra roubo 61
Proteção contra phishing 62
Teclado Virtual....62
O que fazer se você suspeitar que um objeto está infectado com um vírus....63
O que fazer se você suspeitar que o computador está infectado 64
Como restaurar um objeto excluído ou desinfetado pelo aplicativo....66
Como criar e usar o Disco de Recuperação....66
Criando o Disco de Recuperação 66
Inicializando o computador com o Disco de Recuperação 68
Como exibir o relatório de operação do aplicativo....69
Como restaurar as configurações padrão do aplicativo....69
Como importar as configurações do aplicativo Kaspersky Anti-Virus instalado em outro computador....70
Como alternar do Kaspersky Anti-Virus para o Kaspersky Internet Security....71
Alternando para a versão comercial 72
Alternando temporariamente para a versão comercial 72

Como usar o Kaspersky Gadget....73
CONFIGURAÇÕES AVANÇADAS DO APLICATIVO....75
Configurações de proteção geral....76
Restringindo o acesso ao Kaspersky Anti-Virus....76
Selecionando o modo de proteção....77
Verificação....77
Verificação de vírus....77
Verificação de Vulnerabilidades....85
Atualização....85
Selecionando uma fonte de atualização....86
Criando a programação de inicialização da verificação....88
Revertendo a última atualização....89
Verificando a Quarentena após a atualização....89
Usando o servidor proxy....89
Executando atualizações com outra conta de usuário....90
Antivírus de Arquivos....90
Ativando e desativando o Antivírus de Arquivos....91
Pausando o Antivírus de Arquivos automaticamente....91
Criando um escopo de proteção....92
Alterando e restaurando o nível de segurança....93
Selecionando o modo de verificação....93
Usando a análise heurística....94
Selecionando a tecnologia de verificação....94
Alterando as ações a serem executadas com os objetos detectados....94
Verificação de arquivos compostos....95
Otimização da verificação....96
Antivírus de Email....96
Ativando e desativando o Antivírus de Email....97
Criando um escopo de proteção....98
Alterando e restaurando o nível de segurança....98
Usando a análise heurística....99
Alterando as ações a serem executadas com os objetos detectados....99
Filtragem de anexos....99
Verificação de arquivos compostos....100
Verificação de email no Microsoft Office Outlook....100
Verificação de email no The Bat!....100
Antivírus da Web....101
Ativando e desativando o Antivírus da Web....103
Selecionando o nível de segurança do Antivírus da Web....103
Alterando as ações a serem executadas com objetos perigosos....104
Verificando URLs usando os bancos de dados de endereços suspeitos e de phishing....104
Usando a análise heurística....105
Bloqueando scripts perigosos....105
Otimização da verificação....106
Consultor de URLs Kaspersky....106
Criando uma lista de endereços confiáveis....107
Restaurando as configurações padrão do Antivírus da Web....108
Antivírus de IM....108

Ativando e desativando o Antivírus de IM 109
Criando um escopo de proteção 109
Selecionando o método de verificação 109
Defesa Proativa 110
Ativando e desativando a Defesa Proativa 110
Criando um grupo de aplicativos confiáveis 111
Usando a lista de atividades perigosas 111
Alterando a regra de monitoramento de atividades perigosas 111
Inspetor do Sistema 112
Ativando e desativando o Inspetor do Sistema 112
Usando padrões de atividades perigosas (BSS) 113
Revertendo as ações de um programa malicioso 113
Proteção de rede 114
Verificação de conexões criptografadas 114
Configurando o servidor proxy 116
Criando uma lista de portas monitoradas 117
Zona confiável 118
Criando uma lista de aplicativos confiáveis 119
Criando as regras de exclusão 119
Desempenho e compatibilidade com outros aplicativos 119
Selecionando as categorias de ameaças detectáveis 120
Tecnologia de desinfecção avançada 120
Distribuindo os recursos do computador durante a verificação de vírus 121
Executando tarefas em background 121
Configurações do aplicativo no modo de tela inteira. Perfil de Jogo 122
Economia de bateria 122
Autodefesa do Kaspersky Anti-Virus 123
Ativando e desativando a autodefesa 123
Proteção contra o controle externo 123
Quarentena e Backup 124
Armazenando objetos da Quarentena e do Backup 124
Trabalhando com objetos da Quarentena 125
Ferramentas adicionais para proteger melhor seu computador 126
Limpeza de Dados Particulares 127
Configuração do navegador 128
Revertendo as alterações executadas pelos assistentes 130
Relatórios 131
Criando um relatório para o componente selecionado 131
Filtragem de dados 132
Pesquisa de eventos 132
Salvando um relatório em arquivo 133
Armazenando relatórios 133
Limpando os relatórios do aplicativo 134
Registrando eventos não críticos 134
Configurando o lembrete de disponibilidade de relatórios 134
Exibição do aplicativo 135
Capa do aplicativo 135
Elementos ativos da interface 135
Agente de Notícias 135

Notificações 136
Ativando e desativando as notificações 137
Configurando o método de notificação 137
Participando do Kaspersky Security Network 138
VALIDANDO AS CONFIGURAÇÕES DO KASPERSKY ANTI-VIRUS 139
O "vírus" de teste da EICAR e suas modificações 139
Testando a proteção do tráfego HTTP 140
Testando a proteção do tráfego SMTP 141
Validando as configurações do Antivírus de Arquivos 141
Validando as configurações da tarefa de verificação de vírus 142
Validando as configurações do Antispam 142
ENTRANDO EM CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO 143
Minha conta Kaspersky 143
Suporte técnico por telefone 144
Criando um relatório de estado do sistema 144
Criando um arquivo de rastreamento 145
Enviando arquivos de dados 145
Execução do script do AVZ 146
APÊNDICE 148
Status da assinatura 148
Lista de notificações do Kaspersky Anti-Virus 150
Notificações em qualquer modo de proteção 150
Notificações no modo de proteção interativa 155
Trabalhando com o aplicativo na linha de comando 164
Ativando o aplicativo 165
Iniciando o aplicativo 165
Interrompendo o aplicativo 166
Gerenciando componentes e tarefas do aplicativo 166
Verificação de vírus 167
Atualizando o aplicativo 170
Revertendo a última atualização 171
Exportando as configurações de proteção 171
Importando as configurações de proteção 171
Criando um arquivo de rastreamento 172
Exibindo a Ajuda 172
Códigos de retorno da linha de comando 172
GLOSSÁRIO 174
KASPERSKY LAB 184
INFORMAÇÕES SOBRE CÓDIGO DE TERCEIROS 185
Código do programa 185
AGG 2.4 187
ADOBE ABI-SAFE CONTAINERS 1.0 188
BOOST 1.39.0 188
BZIP2/LIBBZIP2 1.0.5 188
CONVERTUTF 188
CURL 7.19.4 189

DEELX - REGULAR EXPRESSION ENGINE 1.2 189
EXPAT 1.2, 2.0.1 189
FASTSCRIPT 1.90 190
FDLIBM 5.3 190
FLEX: THE FAST LEXICAL ANALYZER 2.5.4 190
FMT.H 190
GDTOA 190
GECKO SDK 1.8, 1.9, 1.9.1 191
ICU4C 4.0.1 199
INFO-ZIP 5.51 199
JSON4LUA 0.9.30 200
LIBGD 2.0.35 200
LIBJPEG 6B 201
LIBM (lrint.c v 1.4, lrintf.c,v 1.5) 202
LIBPNG 1.2.8, 1.2.9, 1.2.42 203
LIBUNGIF 3.0 203
LIBXDR 203
LREXLIB 2.4 204
LUA 5.1.4 204
LZMALIB 4.43 205
MD5.H 205
MD5.H 205
MD5-CC 1.02 205
OPENSSL 0.9.8K 206
PCRE 7.7, 7.9 207
SHA1.C 1.2 209
STLPORT 5.2.1 209
SVCCTL.IDL 209
TINYXML 2.5.3 209
VISUAL STUDIO CRT SOURCE CODE 8.0 209
WINDOWS TEMPLATE LIBRARY 8.0 210
ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3 214
Ferramentas de desenvolvimento 214
MS DDK 4.0, 2000 214
MS WDK 6000, 6001, 6002 214
WINDOWS INSTALLER XML (WIX) TOOLSET 3.0 214
Código do programa distribuído 218
GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE) 219
SYSLINUX 3.86 (FILE SYSLINUX.EXE) 223
Outras informações 227
ÍNDICE 228

CONTRATO DE LICENÇA DO USUÁRIO FINAL DA KASPERSKY LAB

IMPORTANTE ADVERTÊNCIA LEGAL PARA TODOS OS USUÁRIOS: LEIAM COM CUIDADO O SEGUINTE CONTRATO LEGAL ANTES DE COMEÇAR A USAR O APLICATIVO.

CLICANDO NO BOTÃO EU CONCORDO NA JANELA DE CONTRATO DE LICENÇA OU AO DIGITAR O(S) SÍMBOLO(S) CORRESPONDENTE(S) VOCÊ ESTARÁ CONCORDANDO EM VINCULAR-SE PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESTA AÇÃO SIMBOLIZA A SUA ASSINATURA E A SUA CONCORDÂNCIA EM VINCULAR-SE PELOS TERMOS DO PRESENTE CONTRATO, TORNANDO-SE PARTE DELE E CONCORDANDO SER ESTE CONTRATO EXECUTÁVEL COMO QUALQUER OUTRO CONTRATO NEGOCIADO E ASSINADO POR VOCÊ**. CASO VOCÊ NÃO CONCORDE COM TODOS OS TERMOS E CONDIÇÕES DO PRESENTE CONTRATO, CANCELE A INSTALAÇÃO DO APLICATIVO E NÃO O INSTALE.

APÓS CLICAR NO BOTÃO EU CONCORDO NA JANELA DE CONTRATO DE LICENÇA OU AO DIGITAR O(S) SÍMBOLO(S) CORRESPONDENTE(S), VOCÊ TERÁ O DIREITO DE USAR O APLICATIVO EM CONFORMIDADE COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

1.1. Aplicativo significa o aplicativo incluindo quaisquer atualizações e materiais relacionados.

1.2. Titular (proprietário de todos os direitos, quer sejam exclusivos ou não ao Aplicativo) significa a Kaspersky Lab ZAO, uma empresa constituída nos termos da legislação da Federação Russa.

1.3. Computador(es) significa(am) equipamento(s), incluindo computadores pessoais, computadores portáteis, estações de trabalho, assistentes digitais pessoais, 'telefones inteligentes', aparelhos de mão ou outros dispositivos eletrônicos para os quais o Aplicativo foi projetado, onde o Aplicativo será instalado e/ou usado.

1.4. Usuário Final (Você / Seu) significa instalação(ões) individual(ais) ou usar o Aplicativo em seu próprio nome ou de quem esteja legalmente usando uma cópia do Aplicativo; ou, se o Aplicativo está sendo baixado ou instalado em nome de uma organização, tal como um empregador, *"Você"* significa ainda a organização para a qual o Aplicativo é baixado ou instalado, declarando-se, para fins do presente instrumento, que tal organização tenha autorizado a pessoa aderindo a este contrato a fazê-lo em seu nome. Para os efeitos do presente documento o termo *"organização"*, inclui, entre outros, qualquer parceria, sociedade de responsabilidade limitada, corporação, associação, sociedade de capital aberto, fundo fiduciário, empreendimento conjunto, organização do trabalho, organização sem personalidade jurídica ou autoridade governamental.

1.5. Parceiro(s) significa organização(ões) ou indivíduo(s) que distribui(em) o Aplicativo, tendo como base um contrato e licenciamento com o Titular.

1.6. Atualização(ões) significa(am) todas as atualizações, revisões, correções, aprimoramentos, emendas, modificações, cópias, adições ou pacotes de manutenção etc.

1.7. Manual do usuário significa manual do usuário, guia do administrador, livro de referência e explicações correlatas ou outros materiais.

2. Licenciamento

2.1. O Titular concede a Você, por este instrumento, uma licença não exclusiva para armazenar, carregar, instalar, executar e exibir ("usar") o Aplicativo em um determinado número de computadores, a fim de ajudar a proteger o seu computador, no qual o Aplicativo é instalado, das ameaças descritas no Manual do usuário, de acordo com todos os requisitos técnicos descritos no Manual do usuário e de acordo com os termos e condições do presente Contrato (a "Licença"), sendo tal Licença aceita por você:

Versão de avaliação. Se tiver recebido, baixado e/ou instalado uma versão de avaliação do Aplicativo e lhe é concedida nesse ato uma licença de avaliação do Aplicativo, você pode usar o Aplicativo apenas para fins de avaliação e apenas durante o único período de avaliação aplicável, salvo indicação contrária, a partir da data da instalação inicial. Qualquer uso do Aplicativo para outros fins ou para além do período de avaliação aplicável é estritamente proibido.

Aplicativo para múltiplos ambientes; Aplicativo para múltiplos idiomas; Aplicativo para mídia dupla; cópias múltiplas; pacotes. Caso você use diferentes versões do Aplicativo ou edições em diferentes idiomas do Aplicativo, caso receba o Aplicativo em múltiplos meios de comunicação, caso receba várias cópias do Aplicativo ou caso tenha recebido o Aplicativo em conjunto com outro aplicativo, o número total permitido dos seus computadores nos quais todas as versões do Aplicativo são instaladas deve corresponder ao número de computadores especificados nas licenças que tenha obtido a partir do Titular, uma vez que, *salvo* se os termos e condições de licenciamento disponham de outra forma, cada licença adquirida lhe dá o direito de instalar e usar o aplicativo em tal número de Computador(es), conforme especificado nas Cláusulas 2.2 e 2.3.

2.2. Caso o Aplicativo tenha sido adquirido por meio físico, Você tem o direito de usar o Aplicativo para a proteção de tal número de Computador(es), conforme especificado no pacote do Aplicativo.

2.3. Caso o Aplicativo tenha sido adquirido na Internet, Você tem o direito de usar o Aplicativo para a proteção de tal número de computadores que foi especificado quando Você adquiriu a licença para o Aplicativo.

2.4. Você tem o direito de fazer uma cópia do Aplicativo apenas para fins de cópia de segurança, e apenas para substituir a cópia legalmente de sua propriedade, caso essa cópia seja extraviada, destruída ou se tornar inutilizável. Tal cópia de segurança não pode ser utilizada para outros fins, devendo ser destruída quando você perder o direito ao uso do Aplicativo ou quando a Sua licença vencer ou for rescindida, por qualquer outro motivo, de acordo com a legislação em vigor no país da sua residência principal ou no país onde Você está usando o Aplicativo.

2.5. Você pode transferir a licença não exclusiva para usar o Aplicativo para outras pessoas físicas no âmbito da licença concedida pelo Titular a Você, desde que o beneficiário concorde em ficar vinculado por todos os termos e condições

deste Contrato e substituí-lo na íntegra na licença concedida pelo Titular. Caso Você transfira integralmente os direitos concedidos pelo Titular para o uso do Aplicativo, Você deve destruir todas as cópias do Aplicativo, incluindo a cópia de segurança. Caso Você seja beneficiário de uma transferência de licença, deverá concordar em obedecer todos os termos e condições deste Contrato. Caso Você não concorde em vincular-se por todos os termos e condições deste Contrato, você não pode instalar e/ou usar o Aplicativo. Você também concorda, na qualidade de beneficiário de uma licença transferida, que Você não tem direitos adicionais ou melhores do que os do usuário final original que adquiriu o aplicativo do Titular.

2.6. A partir do período de ativação do Aplicativo ou após a instalação da licença (com exceção de uma versão de avaliação do Aplicativo) Você tem o direito de receber os seguintes serviços para o período definido especificado no pacote do Aplicativo (caso o Aplicativo tenha sido adquirido em meio físico) ou especificado durante a aquisição (caso o Aplicativo tenha sido adquirido na Internet):

- Atualizações do aplicativo na Internet, quando e como o Titular as publicar em sua página, ou por meio de outros serviços em linha. Quaisquer atualizações que você venha a receber tornam-se parte do Aplicativo, aplicando-se às mesmas os termos e condições do presente Contrato; e

- Assistência técnica na Internet e assistência técnica por linha telefônica direta.

3. Ativação e prazo

3.1. Caso você modifique o seu computador ou faça alterações em aplicativos de outros fornecedores nele instalados, o Titular poderá solicitar que Você repita a ativação do Aplicativo ou instalação da licença. O Titular reserva-se o direito de usar todos os meios e procedimentos de verificação para verificar a validade da Licença e/ou legalidade de cópias do Aplicativo instaladas e/ou usadas em seu computador.

3.2. Caso o Aplicativo tenha sido adquirido em meio físico, o Aplicativo poderá ser usado, mediante aceitação do presente Contrato, durante o período especificado na embalagem, o qual inicia-se após a aceitação do presente Contrato.

3.3. Caso o Aplicativo tenha sido adquirido na Internet, o Aplicativo poderá ser usado, mediante aceitação do presente Contrato, durante o período especificado durante a aquisição.

3.4. Você tem o direito de usar uma versão do Aplicativo, conforme disposto na Cláusula 2.1, sem qualquer encargo, pelo período único de avaliação (30 dias) aplicável a partir do momento de ativação do Aplicativo, de acordo com o presente Contrato, *desde que* a versão de avaliação não lhe conceda nenhum direito a Atualizações e assistência técnica na Internet nem a assistência técnica por linha telefônica direta. Se o Titular determinar outra duração para o período único de avaliação, você será notificado a respeito.

3.5. Sua licença de uso do Aplicativo é restrita ao período de tempo especificado nas Cláusulas 3.2 ou 3.3 (conforme aplicável), e o período restante pode ser visualizado pelo meio descrito no Manual do usuário.

3.6. Se você tiver adquirido o Aplicativo com o objetivo do mesmo ser usado em mais de um Computador, a sua Licença de uso do Aplicativo estará limitada ao período de tempo contado a partir da data de ativação do Aplicativo ou da instalação da licença no primeiro computador.

3.7. Sem prejuízo para quaisquer outras soluções legais ou pelo princípio da equivalência que o Titular possa vir a ter, em caso de qualquer violação de quaisquer termos e condições deste Contrato por Sua parte, o Titular terá, a qualquer momento, sem aviso prévio ao usuário, o direito de rescindir esta Licença para o uso do Aplicativo, sem reembolso do preço de compra ou qualquer parte dele.

3.8. Você concorda que, ao usar o Aplicativo e ao usar qualquer relatório ou informação obtida como resultado da utilização deste Aplicativo, você irá cumprir todas as leis e regulamentos internacionais, nacionais, estaduais, regionais e locais, incluindo, entre outras, as leis de privacidade, do direito autoral, do controle de exportação e a lei sobre obscenidade.

3.9. Salvo se expressamente disposto aqui, você não poderá transferir ou atribuir nenhum dos direitos concedidos ao abrigo deste Contrato ou qualquer uma das suas obrigações relativas ao presente instrumento.

3.10. O Titular de direitos reserva-se o direito de limitar a possibilidade de ativação fora da região na qual o Aplicativo foi adquirido do Titular de direitos e/ou de seus Parceiros.

3.11. Se você tiver adquirido o Aplicativo com código de ativação válido para localização do idioma do Aplicativo da região na qual ele foi adquirido do Titular de direitos ou de seus Parceiros, não poderá ativar o Aplicativo utilizando o código de ativação destinado a outras localizações de idioma.

3.12. No caso das limitações especificadas nas Cláusulas 3.10 e 3.11, as informações sobre essas limitações estão declaradas na embalagem e/ou no site do Titular de direitos e/ou de seus Parceiros.

4. Assistência técnica

4.1. A assistência técnica descrita na Cláusula 2.6 do presente Contrato será fornecida a Você quando a mais recente

atualização do Aplicativo for instalada (com exceção de uma versão de avaliação do Aplicativo).

Serviço de assistência técnica: http://support.kaspersky.com

5. Coleta de informação

5.1. Ao concordar com os termos e condições do presente Contrato, Você estará concordando em prestar informações ao Titular sobre seus arquivos executáveis e suas conferências de número de bits transferidos, com vistas a aprimorar o Seu nível de proteção.

5.2. A fim de melhorar a conscientização da segurança sobre as novas ameaças e as suas fontes, bem como melhorar o Seu nível de proteção de segurança, o Titular, com o seu consentimento, que foi explicitamente confirmado na Declaração de Coleta de Dados de Rede de Segurança da Kaspersky (Kaspersky Security Network Data Collection Statement), tem expressamente o direito de receber tais informações. Você pode desativar o serviço da Rede de Segurança da Kaspersky durante a instalação. Além disso, Você pode ativar e desativar a Rede de Segurança da Kaspersky a qualquer momento na página de opções do Aplicativo.

Além disso, Você reconhece e concorda que qualquer informação recolhida pelo Titular pode ser usada para rastrear e publicar relatórios sobre tendências de riscos de segurança a critério único e exclusivo do Titular.

5.3. O Aplicativo não processa quaisquer dados pessoais identificáveis e não combina dados do processamento com quaisquer informações pessoais.

5.4. Caso você não deseje que as informações coletadas pelo Aplicativo sejam enviadas ao Titular, não deve ativar e/ou desativar o serviço de Rede de Segurança da Kaspersky.

6. Limitações

6.1. Você não deve simular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou fazer engenharia reversa no Aplicativo, nem desmontar ou criar trabalhos derivados do Aplicativo ou de qualquer parte dele, com a única exceção de um direito não renunciável concedido a Você pela legislação aplicável, e você não deve reduzir de nenhuma maneira qualquer parte do Aplicativo para o formato humano legível ou transferir o Aplicativo licenciado ou qualquer subconjunto do Aplicativo licenciado, nem permitir que terceiros o façam, exceto nos casos em que a restrição anterior seja expressamente proibida pela lei aplicável. Nem o código binário do Aplicativo nem o código-fonte pode ser usado ou submetido a engenharia reversa para recriar o algoritmo do programa, que é exclusivo do Titular. Todos os direitos não expressamente concedidos neste Contrato são reservados pelo Titular e/ou seus fornecedores, conforme aplicável. Qualquer uso não autorizado do Aplicativo resultará na rescisão imediata e automática do presente Contrato e da Licença aqui concedida, podendo resultar em processo penal e/ou cível contra Você.

6.2. Você não deve transferir os direitos de uso do Aplicativo a terceiros, salvo conforme estabelecido na Cláusula 2.5 do presente Contrato.

6.3. Você não deve fornecer o código de ativação e/ou o arquivo da chave de licença a terceiros, nem permitir que terceiros tenham acesso ao código de ativação e/ou a chave de licença, os quais são considerados dados confidenciais do Titular, e você tomará todas as precauções, dentro do razoável, para proteger o código de ativação e/ou a chave de licença, de boa-fé, já que você pode transferir o código de ativação e/ou a chave de licença a terceiros, conforme estipulado na Cláusula 2.5 do presente Contrato.

6.4. Você não pode alugar, arrendar ou emprestar o Aplicativo a terceiros.

6.5. Você não deve usar o Aplicativo para a criação de dados ou aplicativos usados para detecção, bloqueio ou tratamento das ameaças descritas no Manual do usuário.

6.6. O Titular tem o direito de bloquear o arquivo da chave ou rescindir a Sua Licença para uso do Aplicativo caso Você viole qualquer dos termos e condições deste Contrato, sem qualquer restituição a Você.

6.7. Caso Você esteja usando a versão de avaliação do Aplicativo, não terá o direito de receber a assistência técnica especificada na Cláusula 4 do presente Contrato, nem terá o direito de transferir a licença ou os direitos de uso do Aplicativo para qualquer terceiro.

7. Garantia restrita e exclusão

7.1. O Titular garante que o Aplicativo irá desempenhar substancialmente, de acordo com as especificações e descrições estabelecidas no Manual do usuário, *desde que, entretanto,* a referida garantia restrita não se aplique ao seguinte: (w) deficiências de seu computador e violação relacionada para as quais o Titular renuncia expressamente a qualquer responsabilidade da garantia; (x) avarias, defeitos ou falhas resultantes de uso indevido, abuso, acidente, negligência, instalação, operação ou manutenção imprópria; furto; vandalismo; atos fortuitos; atos de terrorismo; falhas ou picos de energia; acidente, alteração, modificações ou reparos não permitidos por qualquer terceiro que não seja o Titular, ou quaisquer outros terceiros ou Suas ações ou causas além do controle razoável pelo Titular; (y) qualquer defeito, não divulgado por Você ao Titular o mais rapidamente possível, após o defeito aparecer pela primeira vez; e (z) causados por incompatibilidade de componentes de equipamento e/ou aplicativo instalado em Seu computador.

7.2. Você reconhece, aceita e concorda que nenhum aplicativo está isento de erros, sendo aconselhado a realização de cópia de segurança no computador, com uma frequência e confiabilidade adequadas para Você.

7.3. O Titular não oferece qualquer garantia de que o Aplicativo irá funcionar corretamente em caso de violação dos termos e condições descritos no Manual do usuário ou no presente Contrato.

7.4. O Titular não garante que o Aplicativo irá funcionar corretamente se Você não baixar regularmente as Atualizações especificadas na Cláusula 2.6 do presente Contrato.

7.5. O Titular não garante proteção contra as ameaças descritas no Manual do usuário após o vencimento do prazo especificado nas Cláusulas 3.2 ou 3.3 do presente Contrato ou após a rescisão, por qualquer motivo, da Licença de uso do Aplicativo.

7.6. O APLICATIVO É FORNECIDO "TAL COMO SE ENCONTRA", E O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA QUANTO A SEU USO OU DESEMPENHO. SALVO POR QUALQUER GARANTIA, CONDIÇÃO, DECLARAÇÃO OU TERMO, NA MEDIDA EM QUE NÃO PODE SER EXCLUÍDA OU RESTRITA PELA LEGISLAÇÃO APLICÁVEL, O TITULAR E SEUS PARCEIROS NÃO DÃO NENHUMA GARANTIA, CONDIÇÃO, DECLARAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, USO OU DE ALGUMA OUTRA MANEIRA) QUANTO A QUALQUER ASSUNTO, INCLUINDO, ENTRE OUTROS, A NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS, COMERCIABILIDADE, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE PARA DETERMINADO PROPÓSITO. VOCÊ ASSUME TODAS AS FALHAS E TODO O RISCO QUANTO AO DESEMPENHO E RESPONSABILIDADE DE SELEÇÃO DO APLICATIVO PARA ALCANÇAR SEUS RESULTADOS PRETENDIDOS, BEM COMO PARA A INSTALAÇÃO, USO E RESULTADOS OBTIDOS PELO APLICATIVO. SEM PREJUÍZO DAS DISPOSIÇÕES ANTERIORES, O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA QUE O APLICATIVO ESTARÁ LIVRE DE ERROS, INTERRUPÇÕES OU OUTRAS FALHAS, NEM QUE O APLICATIVO ATENDERÁ QUALQUER OU TODOS OS SEUS REQUISITOS, QUER OU NÃO DIVULGADOS AO TITULAR.

8. Exclusão e limitação da responsabilidade

8.1. NA MEDIDA DO PERMITIDO PELA LEGISLAÇÃO APLICÁVEL, EM NENHUM CASO O TITULAR OU SEUS PARCEIROS SERÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, INCIDENTAIS, PUNITIVOS, INDIRETOS, CONSEQUÊNCIAIS OU QUAISQUER DANOS (INCLUINDO, ENTRE OUTROS, DANOS POR PERDA DE

RECEITA OU CONFIDENCIAIS OU OUTRAS INFORMAÇÕES, POR INTERRUPÇÃO DOS NEGÓCIOS, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANO E PERDA DE DADOS OU PROGRAMAS, POR NÃO CUMPRIMENTO DE QUALQUER DEVER INCLUINDO QUALQUER OBRIGAÇÃO LEGAL, DIREITO DE BOA-FÉ OU DIREITO DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PREJUÍZOS ECONÔMICOS, E QUAISQUER OUTRAS PERDAS PECUNIÁRIAS OU OUTRA PERDA) DECORRENTES DE OU DE ALGUMA MANEIRA RELACIONADOS AO USO OU À IMPOSSIBILIDADE DE USAR O APLICATIVO, A PROVISÃO OU FALTA DE PRESTAÇÃO DE APOIO OU OUTROS SERVIÇOS, INFORMAÇÕES, APLICATIVO E CONTEÚDO RELACIONADO POR MEIO DO APLICATIVO OU DE OUTROS DECORRENTES DO USO DO APLICATIVO OU DE QUALQUER OUTRO RESULTANTE OU RELACIONADO COM QUALQUER DISPOSIÇÃO DO PRESENTE CONTRATO, OU DECORRENTE DE QUALQUER VIOLAÇÃO DE CONTRATO OU QUALQUER OFENSA (INCLUINDO NEGLIGÊNCIA, DETURPAÇÃO, QUALQUER RESPONSABILIDADE OU OBRIGAÇÃO RIGOROSA), OU QUALQUER VIOLAÇÃO DA GARANTIA DE DEVERES ESTATUTÁRIOS OU QUALQUER QUEBRA DA GARANTIA DO TITULAR OU QUALQUER UM DE SEUS PARCEIROS, MESMO SE O TITULAR OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DOS REFERIDOS DANOS.

VOCÊ CONCORDA QUE EM CASO DE O TITULAR E/OU SEUS PARCEIROS SEREM JULGADOS RESPONSÁVEIS, A RESPONSABILIDADE DO TITULAR E/OU DOS SEUS PARCEIROS ESTARÁ RESTRITA AOS CUSTOS DO APLICATIVO. EM NENHUM CASO, A RESPONSABILIDADE DO TITULAR E/OU SEUS PARCEIROS EXCEDERÁ O PREÇO PAGO AO TITULAR OU AO PARCEIRO PELO APLICATIVO (TAL COMO APLICÁVEL).

NADA NESTE CONTRATO EXCLUI OU LIMITA QUALQUER REIVINDICAÇÃO POR MORTE E LESÃO CORPORAL. AINDA NO CASO DE QUALQUER RENÚNCIA, EXCLUSÃO OU RESTRIÇÃO NESTE CONTRATO NÃO PODER SER EXCLUÍDA OU RESTRITA DE ACORDO COM A LEGISLAÇÃO APLICÁVEL, NESSE CASO, APENAS A REFERIDA RENÚNCIA, EXCLUSÃO OU RESTRIÇÃO NÃO IRÁ SE APLICAR A VOCÊ, E VOCÊ CONTINUARÁ VINCULADO POR TODAS AS RENÚNCIAS, EXCLUSÕES E RESTRIÇÕES REMANESCENTES.

9. GNU e outras licenças de terceiros

9.1. O Aplicativo pode incluir alguns programas de aplicativo que são licenciados (ou sublicenciados) para o usuário sob Licença Pública Geral GNU (GNU General Public License, GPL) ou outras licenças similares de aplicativo livre, que, entre outros direitos, permitem ao usuário copiar, modificar e redistribuir determinados programas, ou partes dos mesmos, bem como ter acesso ao código-fonte ("Aplicativo com Código Aberto"). Caso essas licenças exijam que, para qualquer aplicativo que é distribuído a alguém em formato binário executável, o código-fonte também seja disponibilizado a esses usuários, então ele deve ser disponibilizado por meio do envio de uma solicitação para source@kaspersky.com ou o código fonte fornecido juntamente com o Aplicativo. Se quaisquer licenças de Aplicativo com Código Aberto exigirem que o Titular propicie direitos para usar, copiar ou modificar um programa de Aplicativo com Código Aberto que é mais abrangente que os direitos concedidos no presente Contrato, os referidos direitos devem ter primazia sobre os direitos e restrições no presente instrumento.

10. Titularidade da propriedade intelectual

10.1. Você concorda que o Aplicativo e a autoria, sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Aplicativo, são propriedade intelectual e/ou segredos industriais valiosos do Titular ou de seus

parceiros, e que o Titular e seus parceiros, conforme o caso, são protegidos pelo direito civil e penal e pela lei de direitos autorais, segredos industriais, marcas e patentes da Federação Russa, da União Europeia e dos EUA, bem como de outros países e tratados internacionais. O presente Contrato não concede a Você nenhum direito à propriedade intelectual, incluindo todas as marcas comerciais ou marcas de serviço do Titular e/ou seus parceiros ("Marcas"). Você poderá usar as marcas comerciais apenas nas saídas impressas produzidas pelo Aplicativo, de acordo com a prática aceita de marcas comerciais, incluindo a identificação do nome do proprietário da marca comercial. Essa utilização de qualquer marca comercial não lhe dá qualquer direito de propriedade na referida marca. O Titular e/ou seus parceiros possuem e detêm todos os direitos, títulos e interesses relativos ao Aplicativo, incluindo, entre outros, quaisquer correções de erros, melhorias, atualizações ou outras modificações ao Aplicativo, sejam realizadas pelo Titular ou por qualquer terceiro, e todos os direitos autorais, patentes, direitos a segredos comerciais, marcas comerciais e outros direitos de propriedade intelectual contidos neste instrumento. A sua posse, instalação ou uso do Aplicativo não transfere para você qualquer título de propriedade intelectual sobre o Aplicativo, e você não poderá adquirir direitos sobre o Aplicativo, salvo conforme expressamente previsto no presente Contrato. Todas as cópias do Aplicativo feitas em virtude deste instrumento devem conter as mesmas advertências sobre a propriedade que aparecem no Aplicativo. Salvo conforme indicado neste documento, este Contrato não lhe concede direitos de propriedade intelectual ao Aplicativo, e Você reconhece que a Licença, conforme definido mais pormenorizadamente a seguir, concedida ao abrigo do presente Contrato, só lhe garante um direito de uso restrito, nos termos e condições do presente Contrato. O Titular reserva todos os direitos não expressamente concedidos a você no presente Contrato.

10.2. Você concorda em não modificar ou alterar o Aplicativo por qualquer forma. Você não pode remover ou alterar qualquer advertência de direitos autorais ou outras advertências sobre a propriedade de quaisquer cópias do Aplicativo.

11. Lei aplicável; arbitragem

11.1. Este Contrato será regido e interpretado de acordo com as leis da Federação Russa, sem referência a conflitos de leis e princípios. Este Contrato não será regido pela Convenção das Nações Unidas sobre Contratos para a Venda Internacional de Mercadorias, cuja aplicação está expressamente excluída. Qualquer litígio decorrente da interpretação ou aplicação dos termos e condições deste Contrato ou qualquer violação destes deve, se não for resolvida por negociação direita, ser resolvida no Tribunal de Arbitragem Comercial Internacional da Câmara de Comércio e Indústria da Federação Russa em Moscou, Federação Russa. Qualquer adjudicação proferida pelo árbitro será final e vinculativa para as partes, podendo ainda qualquer julgamento sobre tal decisão arbitral ser executado em qualquer tribunal de jurisdição competente. Nada na presente Seção 11 deverá impedir uma Parte de buscar ou obter reparação justa em tribunal competente, quer antes, durante ou depois dos processos de arbitragem.

12. Prazo para interposição de ações judiciais.

12.1. Nenhuma ação, independentemente da forma, decorrente das transações no âmbito do presente Contrato, pode ser interposta por qualquer uma das partes aqui mencionadas após 1 (um) ano de a ação ter ocorrido, ou foi constatado ter ocorrido, salvo ação por violação dos direitos de propriedade intelectual, a qual pode ser instaurada dentro do máximo prazo legal aplicável.

13. Totalidade do contrato; divisibilidade; princípio da não renúncia.

13.1. Este Contrato é o contrato integral entre você e o Titular, substituindo quaisquer outros contratos, propostas, comunicações ou publicidade anterior, sendo verbais ou escritos, com relação ao Aplicativo ou ao objeto do presente Contrato. Você reconhece que leu este Contrato, compreende o mesmo e concorda em vincular-se por seus termos e condições. Caso qualquer disposição do presente Contrato seja constatada por um tribunal de jurisdição competente como inválida, nula ou inexequível, por qualquer motivo, no todo ou em parte, essa disposição será interpretada de maneira mais restritiva para que se torne legal e aplicável, e o Contrato não irá sucumbir em seu todo por conta da mesma, permanecendo o restante do Contrato em plena vigência e efeito até o limite máximo permitido pela lei ou por similitude, preservando simultaneamente, na medida do possível, a sua intenção original. Nenhuma renúncia de qualquer disposição ou condição aqui contida será válida, a menos que seja feita por escrito e assinada por você e por um representante autorizado do Titular, sendo que nenhuma renúncia de qualquer violação de quaisquer disposições do presente Contrato constituirá renúncia quanto a qualquer violação prévia, concomitante ou posterior. A falha por parte do Titular em insistir ou aplicar o desempenho rigoroso de qualquer disposição do presente Contrato ou de qualquer direito não deve ser interpretada como renúncia de qualquer disposição ou direito.

14. Informações para contato do Titular.

Caso tenha quaisquer perguntas relativas a este Contrato, ou caso deseje entrar em contato com o Titular, por qualquer motivo, favor entrar em contato com o nosso Departamento de Atendimento ao Cliente:

Kaspersky Lab ZAO, 10 build. 1 1st Volokolamsky Proezd
Moscou, 123060
Federação Russa

Tel.: +7-495-797-8700
Fax: +7-495-645-7939

Correio eletrônico: info@kaspersky.com

Página na Internet: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Todos os Direitos Reservados. O Aplicativo e qualquer documentação que o acompanha são protegidos pelas leis de direitos autorais e tratados internacionais sobre direitos autorais, bem como outras leis e tratados sobre propriedade intelectual.

SOBRE ESTE MANUAL

Este documento é o Manual para a instalação, configuração e operação do aplicativo Kaspersky Anti-Virus 2011 (aqui chamado de Kaspersky Anti-Virus). O documento foi criado para um público abrangente. É necessário que os usuários do aplicativo consigam operar um computador pessoal em nível básico: estar familiarizados com a interface do sistema operacional Microsoft Windows e em sua navegação, além de saber como usar programas conhecidos de email e Internet, como o Microsoft Office Outlook e o Microsoft Internet Explorer.

O objetivo do documento:

- ajudar os usuários a instalar o aplicativo no computador, ativá-lo e configurar as tarefas desejadas pelo usuário;
- fornecer uma fonte de informações facilmente disponível sobre problemas relacionados ao aplicativo;
- fornecer fontes alternativas de informações sobre o aplicativo e as formas de obter suporte técnico.

NESTA SEÇÃO:

Nesta documentação 18

Convenções da documentação 20

NESTA DOCUMENTAÇÃO

Esta documentação contém as seguintes seções:

Fontes adicionais de informações

Esta seção contém uma descrição dos dados sobre as fontes de informações adicionais referentes ao aplicativo e um recurso na Internet onde é possível discutir o aplicativo, compartilhar ideias, fazer perguntas e obter respostas.

Kaspersky Anti-Virus 2011

Esta seção descreve os novos recursos do aplicativo e fornece informações resumidas sobre seus componentes e suas funções básicas. Ela aborda a função de cada parte do pacote fornecido e uma variedade de serviços disponíveis para os usuários registrados do aplicativo. A seção contém os requisitos de hardware e software que devem ser preenchidos pelo computador para instalar o Kaspersky Anti-Virus.

Instalando e removendo o aplicativo

Esta seção contém instruções que ajudam a instalar o aplicativo no computador ou atualizar a versão anterior. A seção também descreve o procedimento de desinstalação do aplicativo.

Gerenciando a licença

Esta seção contém informações referentes aos conceitos básicos usados no contexto do licenciamento do aplicativo. Nesta seção, você também aprenderá sobre a renovação automática da licença e onde é possível exibir informações referentes à licença atual.

Interface do aplicativo

Esta seção contém uma descrição dos componentes básicos da GUI do aplicativo: ícones e menu de contexto, janela principal do aplicativo, janela de configurações e janelas de notificação.

Iniciando e interrompendo o aplicativo

Esta seção contém informações referentes à execução e ao encerramento do aplicativo.

Status de proteção do computador

Esta seção contém informações sobre como descobrir se o computador está protegido ou se sua segurança está ameaçada, além de como eliminar as ameaças emergentes. Também é possível encontrar informações sobre como ativar, desativar e pausar a proteção ao trabalhar com o Kaspersky Anti-Virus.

Solucionando tarefas típicas

Esta seção contém instruções para as tarefas básicas com as quais a maioria dos usuários se depara ao trabalhar com o aplicativo.

Configurações avançadas do aplicativo

Esta seção fornece informações detalhadas sobre cada componente do aplicativo e descreve os algoritmos de operação e configuração de cada componente.

Verificando a consistência das configurações do aplicativo

Esta seção contém recomendações de como verificar se os componentes do aplicativo estão sendo executados corretamente.

Entrando em contato com o Serviço de Suporte Técnico

Esta seção contém recomendações de como contatar a Kaspersky Lab em Minha conta Kaspersky no site do Serviço de Suporte Técnico e pelo telefone.

Apêndice

Esta seção inclui informações de referência que complementam o texto da documentação.

Glossário

Esta seção contém a lista de termos usados na documentação e suas definições.

CONVENÇÕES DA DOCUMENTAÇÃO

As convenções da documentação usadas neste manual estão descritas na tabela a seguir.

Table 1. Convenções da documentação

TEXTO DE EXEMPLO	DESCRIÇÃO DAS CONVENÇÕES DA DOCUMENTAÇÃO
Observe que...	Os avisos estão realçados em vermelho e dispostos em quadros. Os avisos contêm informações importantes, por exemplo, relacionadas às operações do computador fundamentais para sua segurança.
É recomendável usar...	As observações estão dispostas em quadros. As observações contêm informações adicionais e de referência.
Exemplo: ...	Os exemplos são fornecidos por seção sobre fundo amarelo e sob o título "Exemplo".
Atualização significa...	Os termos novos são realçados em itálico.
ALT+F4	Os nomes de teclas do teclado são exibidos em uma fonte em negrito e em letras maiúsculas. Os nomes das teclas seguidos de um sinal de "adição" indicam o uso de uma combinação de teclas.
Ativar	Os nomes de elementos da interface, como campos de entrada, comandos de menus, botões, etc., são realçados por uma fonte em negrito.
➡ *Para configurar a programação da tarefa:*	As instruções são realçadas pelo símbolo de seta. As frases introdutórias das instruções são exibidas em itálico.
help	Os textos da linha de comando ou de mensagens exibidas na tela utilizam uma fonte especial.
<Endereço IP do computador>	As variáveis são colocadas entre colchetes angulares. Em vez das variáveis, os valores correspondentes são colocados em cada caso e os colchetes angulares são omitidos.

FONTES ADICIONAIS DE INFORMAÇÕES

Se houver dúvidas sobre a escolha, a compra, a instalação ou o uso do Kaspersky Anti-Virus, existem várias fontes de informações disponíveis de acordo com sua conveniência. Você pode escolher a fonte de informações mais adequada de acordo com a importância e a urgência de sua pergunta.

NESTA SEÇÃO:

Fontes de informações para pesquisas independentes 21

Discutindo os aplicativos da Kaspersky no fórum da Web 22

Entrando em contato com o Departamento de vendas 22

Entrando em contato com o grupo de desenvolvimento da Documentação 22

FONTES DE INFORMAÇÕES PARA PESQUISAS INDEPENDENTES

A Kaspersky Lab oferece as seguintes fontes de informações sobre o aplicativo:

- página do aplicativo no site da Kaspersky Lab;
- página do aplicativo no site do Serviço de Suporte Técnico (na Base de Dados de Conhecimento);
- página do Serviço de Suporte do FastTrack
- sistema de Ajuda.

Página do aplicativo no site da Kaspersky Lab

Nesta página (http://brazil.kaspersky.com/products/anti-virus.php) fornece informações gerais sobre o aplicativo, seus recursos e suas opções.

Página do aplicativo no site do Serviço de Suporte Técnico (Base de Dados de Conhecimento)

Nesta página (http://brazil.kaspersky.com/suporte/usuarios-domesticos/anti-virus) você encontra os artigos criados pelos especialistas do Serviço de Suporte Técnico.

Esses artigos contêm informações úteis, recomendações e perguntas frequentes sobre a compra, a instalação e o uso do aplicativo. Eles são classificados por assunto; por exemplo, Gerenciando a licença, Configurando a atualização ou Eliminando falhas de operação. Os artigos podem responder às perguntas referentes a este aplicativo e também a outros produtos da Kaspersky Lab. Eles também podem conter notícias do Serviço de Suporte Técnico.

Serviço de Suporte do FastTrack

Nesta página de serviço, você encontra o banco de dados de perguntas frequentes com respostas referentes à operação do aplicativo. Para usar esse serviço, você precisará de uma conexão com a Internet.

Para ir para a página do serviço, na janela principal do aplicativo, clique no link **Suporte** e, na janela que é aberta, clique no botão **Suporte do FastTrack**.

Sistema de Ajuda

O pacote de instalação do aplicativo inclui o arquivo de Ajuda completa e contextual. Ela contém informações sobre como gerenciar a proteção do computador (exibir o status de proteção, verificar diversas áreas do computador quanto à presença de vírus e executar outras tarefas). O arquivo de Ajuda completa e contextual fornece informações sobre todas as janelas do aplicativo, com a listagem e a descrição das configurações e tarefas relacionadas a cada uma delas.

Para abrir o arquivo de Ajuda, na janela desejada, clique no botão **Ajuda** ou pressione a tecla **F1**.

DISCUTINDO OS APLICATIVOS DA KASPERSKY NO FÓRUM DA WEB

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky Lab e com outros usuários no nosso fórum, em http://forum.kaspersky.com.

Nesse fórum, é possível exibir os tópicos existentes, deixar seus comentários, criar novos tópicos ou usar o mecanismo de pesquisa.

ENTRANDO EM CONTATO COM O DEPARTAMENTO DE VENDAS

Se tiver alguma dúvida sobre como selecionar ou comprar o Kaspersky Anti-Virus ou prorrogar sua licença, entre em contato com o Departamento de Vendas https://store.digitalriver.com/DRHM/servlet/ControllerServlet?Action=DisplayContactFormPage&SiteID=kasperus&Locale=es_BR.

ENTRANDO EM CONTATO COM O GRUPO DE DESENVOLVIMENTO DA DOCUMENTAÇÃO

Se tiver perguntas referentes à documentação, tiver encontrado um erro ou quiser deixar seu feedback, você poderá entrar em contato com o grupo de desenvolvimento da Documentação. Para entrar em contato com o grupo de desenvolvimento da Documentação, envie um email para docfeedback@kaspersky.com. Coloque como assunto da mensagem "Kaspersky Help Feedback: Kaspersky Anti-Virus".

KASPERSKY ANTI-VIRUS 2011

Esta seção descreve os novos recursos do aplicativo e fornece informações resumidas sobre seus componentes e suas funções básicas. Ela aborda a função de cada parte do pacote fornecido e uma variedade de serviços disponíveis para os usuários registrados do aplicativo. A seção contém os requisitos de hardware e software que devem ser preenchidos pelo computador para instalar o Kaspersky Anti-Virus.

NESTA SEÇÃO:

Novidades 23

Assegurando a proteção do computador 23

Kit de distribuição 25

Serviços para usuários registrados 25

Requisitos de hardware e software 26

NOVIDADES

As seguintes inovações foram introduzidas no Kaspersky Anti-Virus:

- O novo componente de proteção Inspetor do Sistema (veja a página 112) monitora a atividade de aplicativos no sistema e fornece informações detalhadas a outros componentes de proteção. Com o histórico de atividades de aplicativos que pode ser recuperado, o componente pode reverter os resultados das ações de um aplicativo malicioso quando elas são detectadas pelos diversos componentes de proteção.

- Com a ajuda da Verificação Ociosa (veja a página 121), o computador pode ser verificado quanto à presença de vírus enquanto você não está trabalhando com ele, e a verificação será interrompida quando você voltar ao trabalho. Isso permite executar verificações periodicamente e, ao mesmo tempo, evita reduzir a velocidade de execução do computador quando você precisa dele.

- Quando o Kaspersky Anti-Virus estiver instalado no computador, você poderá alternar temporariamente para o Kaspersky Internet Security para avaliar seus recursos. Também é possível comprar uma licença para continuar usando o aplicativo. Não será necessário instalar o Kaspersky Internet Security separadamente do Kaspersky Anti-Virus.

- Ao usar o Kaspersky Anti-Virus em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você também pode usar o Kaspersky Gadget (aqui chamado de *gadget*). O Kaspersky Gadget foi criado para acessar rapidamente os principais recursos do aplicativo: indicação de status da proteção, verificação de objetos quanto à presença de vírus, relatórios de operação do aplicativo, etc.

ASSEGURANDO A PROTEÇÃO DO COMPUTADOR

O Kaspersky Anti-Virus oferece proteção abrangente ao seu computador contra ameaças conhecidas e desconhecidas, ataques de rede e de invasores, spam e outras informações indesejadas.

Cada tipo de ameaça é tratada por um *componente de proteção* individual (consulte a descrição dos componentes nesta seção). Os componentes podem ser ativados ou desativados de forma independente e configurados da forma apropriada.

Além da proteção contínua fornecida pelos componentes de segurança, é recomendável *verificar* o computador periodicamente quanto à presença de vírus. Isso é necessário para descartar a possibilidade de disseminação de

programas maliciosos que não foram descobertos pelos componentes de segurança porque, por exemplo, o nível de segurança está com uma definição baixa ou por outros motivos.

Para manter o Kaspersky Anti-Virus atualizado, é necessário *atualizar* os bancos de dados e módulos do aplicativo. O aplicativo é atualizado automaticamente por padrão. Porém, se necessário, você pode atualizar os bancos de dados e módulos do software manualmente a qualquer momento.

Determinadas tarefas específicas que precisam ser realizadas ocasionalmente podem ser executadas com a ajuda de ferramentas e assistentes avançados (consulte a seção "Ferramentas adicionais melhorar a proteção do computador" na página 126), como a configuração do Microsoft Internet Explorer ou a limpeza de rastros de atividades do usuário no sistema.

Componentes de proteção

Os seguintes componentes de proteção protegem o computador em tempo real:

Antivírus de Arquivos

O Antivírus de Arquivos evita a infecção do sistema de arquivos do computador. O componente é executado ao iniciar o sistema operacional, permanece continuamente na RAM do computador e verifica todos os arquivos abertos, gravados ou executados no computador e em todas as unidades conectadas. O Kaspersky Anti-Virus intercepta todas as tentativas de acesso a um arquivo e verifica esse arquivo quanto à presença de vírus conhecidos. O arquivo poderá ser processado somente se não estiver infectado ou for neutralizado com êxito pelo aplicativo. Se por algum motivo o arquivo não puder ser desinfetado, ele será excluído. Uma cópia do arquivo será gravada no backup ou ele será movido para a Quarentena.

Antivírus de Email

O Antivírus de Email verifica os emails enviados e recebidos no computador. O email será disponibilizado ao destinatário somente se não contiver objetos perigosos.

Antivírus da Web

O Antivírus da Web intercepta e bloqueia scripts em sites, caso eles representem uma ameaça. Todo o tráfego da Web também está sujeito a um monitoramento completo. Além disso, o componente bloqueia o acesso a sites maliciosos.

Antivírus de IM

O Antivírus de IM garante o uso seguro de mensagens instantâneas. O componente protege as informações recebidas pelo computador por meio dos protocolos de IM. O Antivírus de IM garante a operação segura de diversos aplicativos de mensagens instantâneas.

Defesa Proativa

A Defesa Proativa permite detectar um novo programa malicioso antes que ele execute sua atividade maliciosa. A operação do componente se baseia no monitoramento e na análise do comportamento de todos os aplicativos instalados no computador. De acordo com as ações executadas, o Kaspersky Anti-Virus decide se o aplicativo é possivelmente perigoso ou não. Assim, o computador fica protegido dos vírus conhecidos e também de vírus novos e daqueles que ainda não foram descobertos.

Antiphishing

Um componente integrado ao Antivírus da Web e ao Antivírus de IM que verifica se os endereços da Web estão incluídos nas listas de endereços de phishing e suspeitos.

Há três grupos de objetos protegidos pelos componentes do aplicativo:

- arquivos, dados de identidade, nomes de usuário e senhas, informações sobre cartões bancários, etc. Esses arquivos são protegidos pelo Antivírus de Arquivos e pela Defesa Proativa.

- Aplicativos instalados no computador e objetos do sistema operacional. Esses arquivos são protegidos pelos componentes Antivírus de Arquivos, Antivírus da Web, Antivírus de IM e Defesa Proativa.

- Atividade online: uso de sistemas de pagamento eletrônico, proteção de email contra spam e vírus, etc. Esses arquivos são protegidos pelos componentes Antivírus de Arquivos, Antivírus da Web, Antivírus de IM e Antiphishing.

O agrupamento dos componentes de acordo com os objetos que protegem está ilustrado graficamente na seção **Centro de Proteção** da janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).

KIT DE DISTRIBUIÇÃO

Você pode adquirir a versão do Kaspersky Anti-Virus na caixa de nossos revendedores ou comprá-la online em lojas da Internet, como a seção **Loja Virtual** em http://brazil.kaspersky.com/comprar/.

Se você comprar a versão do programa na caixa, o pacote incluirá:

- Um envelope lacrado com o CD de instalação contendo os arquivos do programa e a documentação no formato PDF.
- A documentação impressa, especificamente os documentos Manual de Início Rápido e Manual do Usuário (dependendo da região).
- Contrato de Licença (dependendo da região).
- Cartão de ativação com um código de ativação (dependendo da região).

Leia o EULA integralmente com atenção (consulte a seção "Sobre o Contrato de Licença do Usuário Final" na página 39).

Se você não concordar com os termos do EULA, poderá devolver o produto na caixa para o revendedor do qual o comprou e o valor pago pelo programa será reembolsado, desde que o envelope que contém o disco de instalação ainda esteja lacrado.

Ao abrir o disco de instalação lacrado, você aceita todos os termos do EULA.

Antes de romper o lacre do envelope do disco de instalação, leia atentamente o EULA na íntegra.

Se você comprar o Kaspersky Anti-Virus em uma Loja virtual, deverá baixar o produto do site da Kaspersky Lab; este Manual do usuário será fornecido com o pacote de instalação. Você receberá um código de ativação por email após o recebimento do pagamento.

SERVIÇOS PARA USUÁRIOS REGISTRADOS

A Kaspersky Lab oferece aos usuários legalizados um conjunto de serviços que permite aumentar a eficiência de uso do aplicativo.

Quando você compra a licença, se torna um usuário registrado, o que lhe dá o direito de aproveitar os seguintes serviços:

- banco de dados do aplicativo e novas versões do produto atualizados a cada hora;
- consultoria sobre como instalar, configurar e usar o produto por telefone ou no Gabinete Pessoal;
- notificação sobre novos produtos de software lançados pela Kaspersky Lab e novos vírus que surgem em todo o mundo. Este serviço é fornecido aos usuários que assinaram a entrega de notícias da Kaspersky Lab no site do Serviço de Suporte Técnico (http://support.kaspersky.com/subscribe).

Não é fornecida consultoria sobre problemas relacionados ao funcionamento e uso de sistemas operacionais, software de terceiros e tecnologias diversas.

REQUISITOS DE HARDWARE E SOFTWARE

Para o funcionamento correto do Kaspersky Anti-Virus, o computador deve atender a determinados requisitos.

Requisitos gerais:

- 480 MB de espaço em disco disponível.
- CD/DVD-ROM (para instalar o Kaspersky Anti-Virus do CD de instalação).
- Conexão com a Internet (para atualizar os bancos de dados e módulos do aplicativo).
- Microsoft Internet Explorer 6.0 ou superior.
- Microsoft Windows Installer 2.0.

Requisitos para Microsoft Windows XP Home Edition (Service Pack 2 ou superior), Microsoft Windows XP Professional (Service Pack 2 ou superior), Microsoft Windows XP Professional x64 Edition (Service Pack 2 ou superior):

- Processador Intel Pentium 800 MHz 32 bits (x86)/64 bits (x64) ou superior (ou um equivalente compatível);
- 512 MB de RAM livre.

Requisitos para Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- Processador Intel Pentium 1 GHz 32 bits (x86)/64 bits (x64) ou superior (ou um equivalente compatível);

1GB de RAM disponível (32 bits); 2 GB de RAM disponível (64 bits).

Requisitos para netbooks:

- Processador Intel Atom 1.33 MHz (Z520) ou um equivalente compatível.
- Placa de vídeo Intel GMA950 com RAM de vídeo superior a 64 MB (ou um compatível equivalente).
- Tamanho de tela não inferior a 10,1".
- Microsoft Windows XP Home Edition ou superior.

INSTALANDO E REMOVENDO O APLICATIVO

Esta seção contém instruções que ajudam a instalar o aplicativo no computador ou atualizar a versão anterior. A seção também descreve o procedimento de desinstalação do aplicativo.

NESTA SEÇÃO:

Procedimento de instalação padrão 27

Atualizando a versão anterior do Kaspersky Anti-Virus 32

Cenários de instalação diferentes do padrão 36

Iniciando 37

Removendo o aplicativo 37

PROCEDIMENTO DE INSTALAÇÃO PADRÃO

A instalação do Kaspersky Internet Security é executada no computador no modo interativo, usando o Assistente de Instalação.

O Assistente consiste em uma série de telas (etapas) nas quais você navega usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Quando o Kaspersky Anti-Virus estiver instalado no computador, você poderá alternar temporariamente para o Kaspersky Internet Security para avaliar seus recursos. Você também poderá comprar uma licença. Não será necessário instalar o Kaspersky Internet Security separadamente do Kaspersky Anti-Virus.

Se o aplicativo for usado para proteger mais de um computador, ele deverá ser instalado em todos os computadores da mesma forma. Nesse caso, de acordo com o contrato de licença, o período da licença começa na data da primeira ativação.

- *Para instalar o Kaspersky Anti-Virus no computador,*

  execute o arquivo de instalação (um arquivo com a extensão *.exe) do CD do produto.

O processo de instalação do Kaspersky Anti-Virus de um pacote de instalação baixado da Internet é idêntico ao do CD de instalação.

NESTA SEÇÃO:

Etapa 1. Localizando a versão mais recente do aplicativo 28

Etapa 2. Verificando se o sistema atende aos requisitos de instalação 28

Etapa 3. Selecionar o tipo de instalação 29

Etapa 4. Examinando o contrato de licença 29

Etapa 5. Declaração sobre coleta de dados do Kaspersky Security Network 29

Etapa 6. Procurando aplicativos incompatíveis 29

Etapa 7. Selecionando a pasta de destino 30

Etapa 8. Preparando a instalação 30

Etapa 9. Instalando 31

Etapa 10. Ativando o aplicativo 31

Etapa 11. Registrando um usuário 31

Etapa 12. Concluindo a ativação 32

Etapa 13. Conclusão do Assistente 32

ETAPA 1. LOCALIZANDO A VERSÃO MAIS RECENTE DO APLICATIVO

Antes da instalação, o instalador verifica se há uma versão mais recente do Kaspersky Anti-Virus nos servidores de atualização da Kaspersky Lab.

Se não for encontrada nenhuma versão mais recente do produto nos servidores de atualização da Kaspersky Lab, o Assistente de Instalação da versão atual será executado.

Se os servidores de atualização tiverem uma versão mais recente do Kaspersky Anti-Virus, você verá uma solicitação para baixar e instalar essa versão no computador. É recomendável instalar a nova versão do aplicativo, pois as versões mais recentes incluem aprimoramentos que garantem uma proteção mais confiável do computador. Se você cancelar o download da nova verão, o Assistente de Instalação da versão atual será executado. Se você decidir instalar a versão mais recente, os arquivos de distribuição do produto serão baixados no computador e o Assistente de Instalação da nova versão será executado automaticamente. Para obter uma descrição mais detalhada do procedimento de instalação da versão mais recente, consulte a documentação correspondente.

ETAPA 2. VERIFICANDO SE O SISTEMA ATENDE AOS REQUISITOS DE INSTALAÇÃO

Antes da instalação do Kaspersky Anti-Virus no computador, o instalador verifica o sistema operacional e os service packs para confirmar se eles atendem aos requisitos de software para a instalação do produto (consulte a seção "Requisitos de hardware e software" na página 26). Além disso, o instalador verifica a presença dos softwares e das credenciais necessários para instalar aplicativos. Se algum dos requisitos acima não for atendido, será exibida a notificação correspondente na tela.

Se o computador atender a todos os requisitos, o Assistente procurará aplicativos da Kaspersky Lab que, quando executados simultaneamente com o Kaspersky Anti-Virus, podem gerar conflitos. Se forem encontrados aplicativos incompatíveis, será solicitado que você os remova manualmente.

Se for encontrada uma versão anterior do Kaspersky Anti-Virus ou do Kaspersky Internet Security, todos os dados que podem ser usados pelo Kaspersky Anti-Virus 2011 (informações de ativação, configurações do aplicativo, etc.) serão gravadas e usadas ao instalar o novo aplicativo, enquanto o aplicativo anterior será removido automaticamente.

ETAPA 3. SELECIONAR O TIPO DE INSTALAÇÃO

Neste estágio, você pode selecionar o tipo de instalação do Kaspersky Anti-Virus mais adequado:

- *Instalação padrão*. Se você escolher esta opção (a caixa **Alterar configurações de instalação** estará desmarcada), o aplicativo será totalmente instalado no computador com as configurações de proteção recomendadas pela Kaspersky Lab.

- *Instalação personalizada*. Nesse caso (a caixa **Alterar configurações de instalação** está marcada), você poderá especificar a pasta de destino na qual o aplicativo será instalado (consulte a seção "Etapa 7. Selecionando a pasta de destino" na página 30) e desativar a proteção do processo de instalação, se necessário (consulte a seção "Etapa 8. Preparando a instalação" na página 30).

Para continuar a instalação, clique no botão **Avançar**.

ETAPA 4. EXAMINANDO O CONTRATO DE LICENÇA

Nesta etapa, você deve examinar o contrato de licença firmado entre você e a Kaspersky Lab.

Leia o contrato atentamente e, para atestar sua aceitação, clique no botão **Eu concordo**. A instalação continuará.

Se não desejar aceitar o contrato de licença, cancele a instalação do aplicativo clicando no botão **Cancelar**.

ETAPA 5. DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK

Nesta etapa, você será convidado a participar do Kaspersky Security Network. A participação no programa envolve o envio de informações à Kaspersky Lab sobre as novas ameaças detectadas, os aplicativos em execução e os aplicativos assinados baixados no seu computador, juntamente com o ID exclusivo atribuído à sua cópia do Kaspersky Anti-Virus e as informações do seu sistema. Nós asseguramos que nenhum dos seus dados pessoais serão divulgados.

Analise a Declaração Sobre Coleta de Dados do Kaspersky Security Network. Para ler a versão completa da Declaração, clique no botão **Contrato completo do KSN**. Se você concordar todos os itens da declaração, marque a caixa **Eu aceito os termos de participação no Kaspersky Security Network** na janela do Assistente.

Clique no botão **Avançar** ao executar a instalação personalizada (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29). Ao executar a instalação padrão, clique no botão **Instalar**. A instalação continuará.

ETAPA 6. PROCURANDO APLICATIVOS INCOMPATÍVEIS

Nesta etapa, o programa verifica se há aplicativos incompatíveis com o Kaspersky Anti-Virus instalados no computador.

Se não for encontrado nenhum aplicativo incompatível, o Assistente continuará automaticamente na etapa seguinte.

Se forem detectados aplicativos incompatíveis, eles serão exibidos em uma lista na tela e você poderá removê-los. Os aplicativos que não puderem ser removidos automaticamente pelo Kaspersky Anti-Virus deverão ser removidos manualmente. Ao remover os aplicativos incompatíveis, você precisará reiniciar o sistema operacional; em seguida, a instalação do Kaspersky Anti-Virus continuará automaticamente.

Para continuar a instalação, clique no botão **Avançar**.

ETAPA 7. SELECIONANDO A PASTA DE DESTINO

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29). Na instalação padrão, essa etapa é omitida e o aplicativo é instalado na pasta padrão.

Nesta etapa, você poderá selecionar a pasta na qual o Kaspersky Anti-Virus deve ser instalado. O caminho a seguir é definido por padrão:

- **<disco>\Arquivos de Programas\Kaspersky Lab\Kaspersky Anti-Virus 2011** – para sistemas de 32 bits;
- **<disco>\Arquivos de Programas (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2011** – para sistemas de 64 bits.

Para instalar o Kaspersky Anti-Virus em outra pasta, especifique o caminho correspondente no campo de entrada ou clique no botão **Procurar** e selecione uma pasta na janela que é aberta.

Lembre-se das seguintes restrições:

- O aplicativo não pode ser instalado em unidades de rede ou removíveis, nem em unidades virtuais (unidades criadas usando o comando SUBST).
- É recomendável evitar instalar o aplicativo em uma pasta que já contenha arquivos ou outras pastas, pois logo o acesso de edição dessa pasta será bloqueado.
- O caminho da pasta de instalação não pode ter mais de 160 caracteres, nem conter caracteres especiais **/**, **?**, **:**, *****, **"**, **>**, **<** e **|**.

Para saber se há espaço em disco suficiente no computador para instalar o aplicativo, clique no botão **Volume**. Na janela que é aberta, você pode ver as informações de espaço em disco. Para fechar a janela, clique em **OK**.

Para continuar a instalação, clique no botão **Avançar** na janela do Assistente.

ETAPA 8. PREPARANDO A INSTALAÇÃO

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29). Na instalação padrão, essa etapa é ignorada.

Como o computador pode estar infectados com programas maliciosos que podem afetar a instalação do Kaspersky Anti-Virus, o processo de instalação deve ser protegido.

Por padrão, a proteção do processo de instalação está ativada; a caixa **Proteger o processo de instalação** está marcada na janela do Assistente.

Quando não for possível instalar o aplicativo, é recomendável desmarcar essa caixa (por exemplo, ao executar a instalação remota usando a Área de Trabalho Remota do Windows). Talvez o motivo seja essa proteção.

Nesse caso, interrompa a instalação, reinicie-a, marque a caixa **Alterar configurações de instalação** na etapa Selecionar o tipo de instalação (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29) e, na etapa Preparando a instalação, desmarque a caixa **Proteger o processo de instalação**.

Para continuar a instalação, clique no botão **Instalar**.

Ao instalar o aplicativo em um computador com o Microsoft Windows XP, as conexões de rede ativas são interrompidas. A maioria das conexões interrompidas será restaurada após uma pausa.

ETAPA 9. INSTALANDO

A instalação do aplicativo pode levar algum tempo. Aguarde sua conclusão.

Quando a instalação for concluída, o Assistente continuará automaticamente na próxima etapa.

Se ocorrer um erro de instalação decorrente de programas maliciosos que impedem a instalação de aplicativos antivírus no computador, o Assistente de Instalação solicitará que você baixe o *utilitário Ferramenta de Remoção de Vírus Kaspersky* para neutralizar a infecção.

Se concordar em instalar o utilitário, o Assistente de Instalação o baixará dos servidores da Kaspersky Lab e, em seguida, a instalação do utilitário será iniciada automaticamente. Se o Assistente não puder baixar o utilitário, será solicitado que você o faça clicando no link fornecido.

Depois de concluir o trabalho com o utilitário, exclua-o e reinicie a instalação do Kaspersky Anti-Virus.

ETAPA 10. ATIVANDO O APLICATIVO

A *ativação* é o procedimento para ativar a licença que permite usar uma versão totalmente funcional do aplicativo até a expiração da licença.

Você precisará de uma conexão com a Internet para ativar o aplicativo.

Você pode selecionar qualquer das seguintes opções ao ativar o Kaspersky Anti-Virus:

- **Ativar a versão comercial**. Se tiver comprado a versão comercial do aplicativo, selecione esta opção e insira o código de ativação (consulte a seção "Sobre o código de ativação" na página 40).

  Se você inserir o código do Kaspersky Internet Security no campo de entrada, ao concluir a ativação será iniciado um procedimento que permite alternar para o Kaspersky Internet Security.

- **Ativar versão de avaliação**. Use esta opção de ativação se desejar instalar a versão de avaliação do aplicativo antes de decidir comprar a versão comercial. Você poderá usar a versão totalmente funcional do aplicativo durante o período limitado pela licença da versão de avaliação do aplicativo. Quando a licença expirar, ela não poderá ser ativada pela segunda vez.

- **Ativar mais tarde**. Se você escolher esta opção, o estágio de ativação do Kaspersky Anti-Virus será ignorado. O aplicativo será instalado no computador com todas as funções disponíveis, exceto as atualizações. Você poderá atualizar os bancos de dados de antivírus e os módulos do Kaspersky Anti-Virus apenas uma vez após a instalação. A opção **Ativar mais tarde** estará disponível somente ao iniciar o Assistente de Ativação pela primeira vez, imediatamente após a instalação do aplicativo.

ETAPA 11. REGISTRANDO UM USUÁRIO

Esta etapa está disponível somente ao ativar a versão comercial do aplicativo. Na ativação da versão de avaliação, essa etapa é ignorada.

É necessário se registrar para poder entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab no futuro.

Se você concordar em se registrar, especifique a data do registro nos campos correspondentes e clique no botão **Avançar**.

ETAPA 12. CONCLUINDO A ATIVAÇÃO

O Assistente informará que o Kaspersky Anti-Virus foi ativado com êxito. Além disso, são fornecidas informações sobre a licença: o tipo de licença (comercial ou avaliação), a data de expiração e o número de hosts com a licença.

Se você tiver ativado a assinatura, serão exibidas informações sobre o status da assinatura (consulte a seção "Status da assinatura" na página 148) em vez da data de expiração da licença.

Clique no botão **Avançar** para continuar com o Assistente.

ETAPA 13. CONCLUSÃO DO ASSISTENTE

A última janela do Assistente informa sobre a conclusão bem-sucedida da instalação do aplicativo. Para executar o Kaspersky Anti-Virus, confirme se a caixa **Executar o Kaspersky Anti-Virus** está marcada e clique no botão **Concluir**.

Em alguns casos, pode ser necessário reiniciar o sistema operacional. Se a caixa **Executar o Kaspersky Anti-Virus** estiver marcada, o aplicativo será executado automaticamente após a reinicialização do sistema operacional.

Se você tiver desmarcado a caixa antes de fechar o Assistente, execute o aplicativo manualmente (consulte a seção "Iniciando e interrompendo o aplicativo manualmente" na página 50).

ATUALIZANDO A VERSÃO ANTERIOR DO KASPERSKY ANTI-VIRUS

Se o Kaspersky Anti-Virus 2010 já estiver instalado no computador, atualize o aplicativo para o Kaspersky Anti-Virus 2011. Se você tiver uma licença ativa do Kaspersky Anti-Virus 2010, não será necessário ativar o aplicativo: o Assistente de Instalação receberá as informações da licença do Kaspersky Anti-Virus 2010 automaticamente para usá-las durante o processo de instalação.

A instalação do Kaspersky Internet Security é executada no computador no modo interativo, usando o Assistente de Instalação.

O Assistente consiste em uma série de telas (etapas) nas quais você navega usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Quando o Kaspersky Anti-Virus estiver instalado no computador, você poderá alternar temporariamente para o Kaspersky Internet Security para avaliar seus recursos. Também é possível comprar uma licença para continuar usando o aplicativo. Não será necessário instalar o Kaspersky Internet Security separadamente do Kaspersky Anti-Virus.

Se o aplicativo for usado para proteger mais de um computador, ele deverá ser instalado em todos os computadores da mesma forma. Nesse caso, de acordo com o contrato de licença, o período da licença começa na data da primeira ativação.

- *Para instalar o Kaspersky Anti-Virus no computador,*

  execute o arquivo de instalação (um arquivo com a extensão *.exe) do CD do produto.

  O processo de instalação do Kaspersky Anti-Virus de um pacote de instalação baixado da Internet é idêntico ao do CD de instalação.

NESTA SEÇÃO:

Etapa 1. Localizando a versão mais recente do aplicativo 33

Etapa 2. Verificando se o sistema atende aos requisitos de instalação 33

Etapa 3. Selecionar o tipo de instalação 34

Etapa 4. Examinando o contrato de licença 34

Etapa 5. Declaração sobre coleta de dados do Kaspersky Security Network 34

Etapa 6. Procurando aplicativos incompatíveis 34

Etapa 7. Selecionando a pasta de destino 35

Etapa 8. Preparando a instalação 35

Etapa 9. Instalando 36

Etapa 10. Concluindo a ativação 36

Etapa 11. Conclusão do Assistente 36

ETAPA 1. LOCALIZANDO A VERSÃO MAIS RECENTE DO APLICATIVO

Antes da instalação, o instalador verifica se há uma versão mais recente do Kaspersky Anti-Virus nos servidores de atualização da Kaspersky Lab.

Se não for encontrada nenhuma versão mais recente do produto nos servidores de atualização da Kaspersky Lab, o Assistente de Instalação da versão atual será executado.

Se os servidores de atualização tiverem uma versão mais recente do Kaspersky Anti-Virus, você verá uma solicitação para baixar e instalar essa versão no computador. É recomendável instalar a nova versão do aplicativo, pois as versões mais recentes incluem aprimoramentos que garantem uma proteção mais confiável do computador. Se você cancelar o download da nova verão, o Assistente de Instalação da versão atual será executado. Se você decidir instalar a versão mais recente, os arquivos de distribuição do produto serão baixados no computador e o Assistente de Instalação da nova versão será executado automaticamente. Para obter uma descrição mais detalhada do procedimento de instalação da versão mais recente, consulte a documentação correspondente.

ETAPA 2. VERIFICANDO SE O SISTEMA ATENDE AOS REQUISITOS DE INSTALAÇÃO

Antes da instalação do Kaspersky Anti-Virus no computador, o instalador verifica o sistema operacional e os service packs para confirmar se eles atendem aos requisitos de software para a instalação do produto (consulte a seção "Requisitos de hardware e software" na página 26). Além disso, o instalador verifica a presença dos softwares e das credenciais necessários para instalar aplicativos. Se algum dos requisitos acima não for atendido, será exibida a notificação correspondente na tela.

Se o computador atender a todos os requisitos, o Assistente procurará aplicativos da Kaspersky Lab que, quando executados simultaneamente com o Kaspersky Anti-Virus, podem gerar conflitos. Se forem encontrados aplicativos incompatíveis, será solicitado que você os remova manualmente.

Se for encontrada uma versão anterior do Kaspersky Anti-Virus ou do Kaspersky Internet Security, todos os dados que podem ser usados pelo Kaspersky Anti-Virus 2011 (informações de ativação, configurações do aplicativo, etc.) serão gravadas e usadas ao instalar o novo aplicativo, enquanto o aplicativo anterior será removido automaticamente.

ETAPA 3. SELECIONAR O TIPO DE INSTALAÇÃO

Neste estágio, você pode selecionar o tipo de instalação do Kaspersky Anti-Virus mais adequado:

- *Instalação padrão*. Se você escolher esta opção (a caixa **Alterar configurações de instalação** estará desmarcada), o aplicativo será totalmente instalado no computador com as configurações de proteção recomendadas pela Kaspersky Lab.

- *Instalação personalizada*. Nesse caso (a caixa **Alterar configurações de instalação** está marcada), você poderá especificar a pasta de destino na qual o aplicativo será instalado (consulte a seção "Etapa 7. Selecionando a pasta de destino" na página 30) e desativar a proteção do processo de instalação, se necessário (consulte a seção "Etapa 8. Preparando a instalação" na página 30).

Para continuar a instalação, clique no botão **Avançar**.

ETAPA 4. EXAMINANDO O CONTRATO DE LICENÇA

Nesta etapa, você deve examinar o contrato de licença firmado entre você e a Kaspersky Lab.

Leia o contrato atentamente e, para atestar sua aceitação, clique no botão **Eu concordo**. A instalação continuará.

Se não desejar aceitar o contrato de licença, cancele a instalação do aplicativo clicando no botão **Cancelar**.

ETAPA 5. DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK

Nesta etapa, você será convidado a participar do Kaspersky Security Network. A participação no programa envolve o envio de informações à Kaspersky Lab sobre as novas ameaças detectadas, os aplicativos em execução e os aplicativos assinados baixados no seu computador, juntamente com o ID exclusivo atribuído à sua cópia do Kaspersky Anti-Virus e as informações do seu sistema. Nós asseguramos que nenhum dos seus dados pessoais serão divulgados.

Analise a Declaração Sobre Coleta de Dados do Kaspersky Security Network. Para ler a versão completa da Declaração, clique no botão **Contrato completo do KSN**. Se você concordar todos os itens da declaração, marque a caixa **Eu aceito os termos de participação no Kaspersky Security Network** na janela do Assistente.

Clique no botão **Avançar** ao executar a instalação personalizada (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29). Ao executar a instalação padrão, clique no botão **Instalar**. A instalação continuará.

ETAPA 6. PROCURANDO APLICATIVOS INCOMPATÍVEIS

Nesta etapa, o programa verifica se há aplicativos incompatíveis com o Kaspersky Anti-Virus instalados no computador.

Se não for encontrado nenhum aplicativo incompatível, o Assistente continuará automaticamente na etapa seguinte.

Se forem detectados aplicativos incompatíveis, eles serão exibidos em uma lista na tela e você poderá removê-los. Os aplicativos que não puderem ser removidos automaticamente pelo Kaspersky Anti-Virus deverão ser removidos manualmente. Ao remover os aplicativos incompatíveis, você precisará reiniciar o sistema operacional; em seguida, a instalação do Kaspersky Anti-Virus continuará automaticamente.

Para continuar a instalação, clique no botão **Avançar**.

ETAPA 7. SELECIONANDO A PASTA DE DESTINO

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29). Na instalação padrão, essa etapa é omitida e o aplicativo é instalado na pasta padrão.

Nesta etapa, você poderá selecionar a pasta na qual o Kaspersky Anti-Virus deve ser instalado. O caminho a seguir é definido por padrão:

- **<disco>\Arquivos de Programas\Kaspersky Lab\Kaspersky Anti-Virus 2011** – para sistemas de 32 bits;
- **<disco>\Arquivos de Programas (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2011** – para sistemas de 64 bits.

Para instalar o Kaspersky Anti-Virus em outra pasta, especifique o caminho correspondente no campo de entrada ou clique no botão **Procurar** e selecione uma pasta na janela que é aberta.

Lembre-se das seguintes restrições:

- O aplicativo não pode ser instalado em unidades de rede ou removíveis, nem em unidades virtuais (unidades criadas usando o comando SUBST).
- É recomendável evitar instalar o aplicativo em uma pasta que já contenha arquivos ou outras pastas, pois logo o acesso de edição dessa pasta será bloqueado.
- O caminho da pasta de instalação não pode ter mais de 160 caracteres, nem conter caracteres especiais **/**, **?**, **:**, *****, **"**, **>**, **<** e **|**.

Para saber se há espaço em disco suficiente no computador para instalar o aplicativo, clique no botão **Volume**. Na janela que é aberta, você pode ver as informações de espaço em disco. Para fechar a janela, clique em **OK**.

Para continuar a instalação, clique no botão **Avançar** na janela do Assistente.

ETAPA 8. PREPARANDO A INSTALAÇÃO

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29). Na instalação padrão, essa etapa é ignorada.

Como o computador pode estar infectados com programas maliciosos que podem afetar a instalação do Kaspersky Anti-Virus, o processo de instalação deve ser protegido.

Por padrão, a proteção do processo de instalação está ativada; a caixa **Proteger o processo de instalação** está marcada na janela do Assistente.

Quando não for possível instalar o aplicativo, é recomendável desmarcar essa caixa (por exemplo, ao executar a instalação remota usando a Área de Trabalho Remota do Windows). Talvez o motivo seja essa proteção.

Nesse caso, interrompa a instalação, reinicie-a, marque a caixa **Alterar configurações de instalação** na etapa Selecionar o tipo de instalação (consulte a seção "Etapa 3. Selecionar o tipo de instalação" na página 29) e, na etapa Preparando a instalação, desmarque a caixa **Proteger o processo de instalação**.

Para continuar a instalação, clique no botão **Instalar**.

Ao instalar o aplicativo em um computador com o Microsoft Windows XP, as conexões de rede ativas são interrompidas. A maioria das conexões interrompidas será restaurada após uma pausa.

ETAPA 9. INSTALANDO

A instalação do aplicativo pode levar algum tempo. Aguarde sua conclusão.

Quando a instalação for concluída, o Assistente continuará automaticamente na próxima etapa.

Se ocorrer um erro de instalação decorrente de programas maliciosos que impedem a instalação de aplicativos antivírus no computador, o Assistente de Instalação solicitará que você baixe o *utilitário Ferramenta de Remoção de Vírus Kaspersky* para neutralizar a infecção.

Se concordar em instalar o utilitário, o Assistente de Instalação o baixará dos servidores da Kaspersky Lab e, em seguida, a instalação do utilitário será iniciada automaticamente. Se o Assistente não puder baixar o utilitário, será solicitado que você o faça clicando no link fornecido.

Depois de concluir o trabalho com o utilitário, exclua-o e reinicie a instalação do Kaspersky Anti-Virus.

ETAPA 10. CONCLUINDO A ATIVAÇÃO

O Assistente informará que o Kaspersky Anti-Virus foi ativado com êxito. Além disso, são fornecidas informações sobre a licença: o tipo de licença (comercial ou avaliação), a data de expiração e o número de hosts com a licença.

Se você tiver ativado a assinatura, serão exibidas informações sobre o status da assinatura (consulte a seção "Status da assinatura" na página 148) em vez da data de expiração da licença.

Clique no botão **Avançar** para continuar com o Assistente.

ETAPA 11. CONCLUSÃO DO ASSISTENTE

A última janela do Assistente informa sobre a conclusão bem-sucedida da instalação do aplicativo. Para executar o Kaspersky Anti-Virus, confirme se a caixa **Executar o Kaspersky Anti-Virus** está marcada e clique no botão **Concluir**.

Em alguns casos, pode ser necessário reiniciar o sistema operacional. Se a caixa **Executar o Kaspersky Anti-Virus** estiver marcada, o aplicativo será executado automaticamente após a reinicialização do sistema operacional.

Se você tiver desmarcado a caixa antes de fechar o Assistente, execute o aplicativo manualmente (consulte a seção "Iniciando e interrompendo o aplicativo manualmente" na página 50).

CENÁRIOS DE INSTALAÇÃO DIFERENTES DO PADRÃO

Esta seção descreve cenários de instalação do aplicativo diferentes da instalação padrão ou da atualização da versão anterior.

Instalando o Kaspersky Anti-Virus com a ativação usando um código de ativação do Kaspersky Internet Security

Se, ao instalar o Kaspersky Anti-Virus, na etapa Ativando o aplicativo, você inserir um código de ativação do Kaspersky Internet Security, o procedimento de expansão será iniciado, resultando na instalação do Kaspersky Internet Security no computador.

Se, ao instalar o Kaspersky Anti-Virus, na etapa Ativando o aplicativo, você selecionar **Ativar mais tarde** e ativar o aplicativo usando um código de ativação do Kaspersky Internet Security, o procedimento de expansão também será iniciado, resultando na instalação do Kaspersky Internet Security no computador.

Instalando o Kaspersky Anti-Virus 2011 sobre o Kaspersky Internet Security 2010

Se você executar a instalação do Kaspersky Anti-Virus 2011 em um computador em que o Kaspersky Internet Security 2010 com uma licença ativa já estiver instalado, o Assistente de Instalação detectará as informações da licença e permitirá que você selecione uma das seguintes ações:

- Usar a licença atual do Kaspersky Internet Security 2010. Nesse caso, o procedimento de expansão será iniciado, resultando na instalação do Kaspersky Internet Security 2011 no computador. Você poderá usar o Kaspersky Internet Security 2011 enquanto a licença do Kaspersky Internet Security 2010 for válida.

- Continuar a instalação do Kaspersky Anti-Virus 2011. Nesse caso, o procedimento de instalação continuará de acordo com o cenário padrão, a partir da etapa Ativando o aplicativo.

INICIANDO

Após a instalação, o aplicativo está pronto para ser usado. Para garantir a proteção adequada do computador, é recomendável executar o seguinte imediatamente após a instalação e configuração:

- Atualizar os bancos de dados do aplicativo (consulte a seção "Como atualizar os bancos de dados e módulos do aplicativo" na página 57).

- Verificar o computador quanto à presença de vírus (consulte a seção "Como executar a verificação completa do computador quanto à presença de vírus" na página 60) e vulnerabilidades (consulte a seção "Verificando vulnerabilidades no computador" na página 61).

- Verifique o status de proteção do computador (na página 51) e elimine os problemas de proteção, se necessário (consulte a seção "Diagnóstico e eliminação de problemas na proteção do computador" na página 51).

REMOVENDO O APLICATIVO

Depois que o Kaspersky Anti-Virus for desinstalado, o computador e seus dados pessoais estarão desprotegidos.

Você pode desinstalar o Kaspersky Anti-Virus usando o Assistente de Instalação.

Para iniciar o Assistente:

1. No menu **Iniciar**, selecione **Programas** → **Kaspersky Anti-Virus 2011** → **Reparar ou Remover**.

2. Na janela que é aberta, clique no botão **Remover**.

NESTA SEÇÃO:

Etapa 1. Salvando dados para usar novamente 37

Etapa 2. Confirmação da remoção do aplicativo 38

Etapa 3. Removendo o aplicativo Concluindo a remoção 38

ETAPA 1. SALVANDO DADOS PARA USAR NOVAMENTE

Neste momento, é possível especificar os dados usados pelo aplicativo que você deseja manter para usar novamente na próxima instalação do aplicativo (por exemplo, uma versão mais nova do aplicativo).

Por padrão, o aplicativo é removido completamente do computador.

Para salvar os dados para usar novamente:

1. Selecione **Salvar objetos do aplicativo**.

2. Marque as caixas ao lado dos tipos de dados que deseja salvar:

   - **Dados de ativação** – dados que eliminam a necessidade de ativar o aplicativo futuramente através do uso automático da licença atual, desde que ela não expire até o momento da próxima instalação.

   - **Bancos de dados do Antispam** – bancos de dados que contêm assinaturas de mensagens de spam baixadas e gravadas pelo aplicativo.

   - **Arquivos do Backup e da Quarentena** – arquivos verificados pelo aplicativo e colocados no armazenamento de Backup ou na Quarentena.

   - **Configurações de operação do aplicativo** – valores das configurações do aplicativo selecionadas durante sua configuração.

   - **Dados do iSwift e do iChecker** – arquivos que contêm informações sobre os objetos que já foram verificados quanto à presença de vírus.

   - **Dados da pasta compartilhada da Execução Segura** – arquivos gravados pelo aplicativo ao trabalhar em um ambiente seguro em uma pasta especial que também pode ser acessada no ambiente normal.

ETAPA 2. CONFIRMAÇÃO DA REMOÇÃO DO APLICATIVO

Como a remoção do aplicativo ameaça a segurança do computador e de seus dados pessoais, será solicitado que você confirme sua intenção de remover o aplicativo. Para fazer isso, clique no botão **Remover**.

Para interromper a remoção do aplicativo a qualquer momento, a operação pode ser cancelada clicando no botão **Cancelar**.

ETAPA 3. REMOVENDO O APLICATIVO CONCLUINDO A REMOÇÃO

Nesta etapa, o Assistente remove o aplicativo do computador. Aguarde a conclusão da remoção.

Ao remover o aplicativo, talvez seja necessário reiniciar o sistema operacional. Se você cancelar a reinicialização imediata, a conclusão do procedimento de remoção será adiada até que o sistema operacional seja reiniciado ou o computador seja desligado e reiniciado.

GERENCIANDO A LICENÇA

Esta seção contém informações referentes aos conceitos básicos usados no contexto do licenciamento do aplicativo. Nesta seção, você também aprenderá sobre a renovação automática da licença e onde é possível exibir informações referentes à licença atual.

NESTA SEÇÃO:

Sobre o Contrato de Licença do Usuário Final 39

Sobre a licença 39

Sobre o código de ativação 40

Exibindo informações da licença 40

SOBRE O CONTRATO DE LICENÇA DO USUÁRIO FINAL

Contrato de Licença do Usuário Final – é um contrato entre pessoas físicas ou jurídicas que têm a posse legal de uma cópia do aplicativo. O EULA é fornecido com todos os aplicativos da Kaspersky Lab. Ele contém uma descrição detalhada dos direitos e das restrições de uso do Kaspersky Anti-Virus.

De acordo com o EULA, quando você compra e instala um aplicativo da Kaspersky Lab, obtém o direito ilimitado de possuir sua cópia.

SOBRE A LICENÇA

Licença é o direito de usar o Kaspersky Anti-Virus e os serviços adicionais relacionados oferecido pela Kaspersky Lab ou por seus parceiros.

Cada licença é definida por sua data de expiração e seu tipo.

Período da licença – o período durante o qual os serviços adicionais são fornecidos:

- suporte técnico;
- atualização dos bancos de dados e módulos do aplicativo.

Os serviços fornecidos dependem do tipo de licença.

São oferecidos os seguintes tipos de licença:

- *Avaliação* – uma licença gratuita com período de validade limitado, por exemplo, 30 dias, oferecida para você se familiarizar como Kaspersky Anti-Virus.

  A licença de avaliação pode ser usada apenas uma vez e não pode ser usada após a licença comercial.

  Uma licença de avaliação é fornecida com a versão de avaliação do aplicativo. Se você tiver uma licença de avaliação, poderá entrar em contato com o Serviço de Suporte Técnico somente para dúvidas referentes à ativação do produto ou à compra de uma licença comercial. Assim que a licença de avaliação expirar, todos os recursos do Kaspersky Anti-Virus serão desativados. Para continuar usando o aplicativo, é necessário ativá-lo (consulte a seção "Como ativar o aplicativo" na página 55).

- *Comercial* – uma licença comercial com período de validade limitado (por exemplo, um ano), oferecida na compra do Kaspersky Anti-Virus. Uma licença pode servir vários computadores.

  Se uma licença comercial for ativada, todos os recursos e serviços adicionais do aplicativo estarão disponíveis.

  Quando a licença comercial expirar, o Kaspersky Anti-Virus continuará sendo um aplicativo com todos os recursos, mas os bancos de dados de antivírus não serão atualizados. Você ainda poderá verificar o computador quanto à presença de vírus e usar os componentes de proteção, mas apenas com os bancos de dados que você tinha quando a licença expirou. Duas semanas antes da data de expiração da licença, o aplicativo o notificará sobre esse evento, de forma que você possa renovar a licença antecipadamente (consulte a seção "Como comprar ou renovar a licença" na página 56).

- *Comercial com assinatura de atualização* e *comercial com assinatura de atualização e proteção* – uma licença paga com gerenciamento flexível: você pode suspender e reiniciar a assinatura, estender seu período de validade no modo automático e cancelar a assinatura. As licenças com assinatura são distribuídas por provedores de serviços. Você pode gerenciar a assinatura no Gabinete Pessoal do usuário no site do provedor de serviços.

  O período de validade de uma assinatura pode ser limitado (por exemplo, um ano) ou ilimitado. Se uma assinatura com um período de validade limitado estiver ativada, você mesmo deverá renová-la quando ela expirar. A assinatura com período de validade ilimitado é estendida automaticamente, estando sujeita ao pré-pagamento oportuno ao provedor.

  Se a vigência da assinatura for limitada, quando ela expirar, você poderá obter um período de tolerância para a renovação da assinatura, durante o qual a funcionalidade completa do programa será mantida.

  Se a assinatura for renovada, quando o período de tolerância expirar, o Kaspersky Anti-Virus interromperá a atualização dos bancos de dados do aplicativo (para a licença com assinatura de atualização) e interromperá a proteção do computador e a execução das tarefas de verificação (para a licença com assinatura de proteção).

  Ao usar a assinatura, você não poderá usar outro código de ativação para renovar a licença. Isso será possível somente após a data de expiração da assinatura.

  Se você já tiver uma licença ativada com período limitado no momento da ativação da assinatura, ela será substituída pela licença de assinatura. Para cancelar a assinatura, entre em contato com o provedor de serviços do qual você comprou o Kaspersky Anti-Virus.

  Dependendo do provedor de assinaturas, o conjunto de ações disponíveis para execução na assinatura (consulte a seção "Status da assinatura" na página 148) podem variar. Além disso, o período de tolerância no qual a renovação da licença está disponível não é fornecido por padrão.

SOBRE O CÓDIGO DE ATIVAÇÃO

O *código de ativação* é um código fornecido com a licença comercial do Kaspersky Anti-Virus. Esse código é necessário para a ativação do aplicativo.

O código de ativação consiste em uma sequência de caracteres e dígitos do alfabeto latino separados por hifens em quatro grupos de cinco símbolos, sem espaços. Por exemplo, 11111-11111-11111-11111.

EXIBINDO INFORMAÇÕES DA LICENÇA

➧ *Para exibir informações sobre a licença ativa:*

1. Abra a janela principal do aplicativo.

2. Clique no botão **Licença** na parte inferior da janela para abrir a janela **Gerenciamento de licenças**.

Nesta janela, você pode iniciar a ativação do aplicativo (consulte a seção "Como ativar o aplicativo" na página 55), comprar uma nova licença ou renovar a licença atual (consulte a seção "Como comprar ou renovar a licença" na página 56).

Gerenciamento de licenças
0F92-000534-08CEBA68
Ativo
Comercial para 1 computador para 30 dias
Válido de 21.07.2010 a 17.08.2010 23:59:59
27 dias restantes.
Renovar licença
Visitar a Loja virtual para renovar a licença
Ativar o aplicativo com uma nova licença
Executar o Assistente de Ativação do Kaspersky Anti-Virus
Ajuda
Exibir Contrato de licença do usuário final
Fechar

Figura 1. A janela Gerenciamento de licenças

INTERFACE DO APLICATIVO

O Kaspersky Anti-Virus possui uma interface bastante simples e fácil de usar. Nesta seção, abordaremos detalhadamente seus recursos básicos.

O Kaspersky Anti-Virus inclui componentes de extensão (plug-ins) para os programas Microsoft Office Outlook, Microsoft Outlook Express, The Bat!, Thunderbird, Mozilla Firefox, Microsoft Internet Explorer e Microsoft Windows Explorer. Os plug-ins ampliam a funcionalidade dos aplicativos host, dando acesso à configuração dos componentes do produto em suas interfaces.

NESTA SEÇÃO:

Ícone da área de notificação 42

Menu de contexto 43

Janela principal do Kaspersky Anti-Virus 44

Janelas de notificação e mensagens pop-up 46

Janela de configuração do aplicativo 48

Kaspersky Gadget 49

ÍCONE DA ÁREA DE NOTIFICAÇÃO

Imediatamente após a instalação do Kaspersky Anti-Virus, o ícone do aplicativo aparecerá na área de notificação da barra de tarefas do Microsoft Windows.

Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

O ícone tem as seguintes finalidades básicas:

- É um indicador da operação do aplicativo.
- Dá acesso ao menu de contexto, à janela principal do aplicativo e a janela de notícias.

Indicação da atividade do aplicativo

Esse ícone é um indicador da operação do aplicativo. Ele também indica o status da proteção e mostra várias funções básicas executadas pelo aplicativo no momento:

– verificação de mensagens de email;

– verificação do tráfego da Web;

– atualização os bancos de dados e módulos do aplicativo;

– o computador deve ser reiniciado para aplicar as atualizações;

– ocorreu uma falha na operação de algum componente do aplicativo.

Por padrão, o ícone é animado: por exemplo, durante a verificação dos emails, um pequeno símbolo de carta pisca no ícone do aplicativo; quando a atualização está em andamento, é possível ver um globo girando. Você pode desativar a animação (consulte a seção "Elementos ativos da interface" na página 135).

Quando a animação é desativada, o ícone pode ter as seguintes formas:

(símbolo colorido) – todos ou determinados componentes de proteção são ativados;

(símbolo preto e branco) – todos os componentes de proteção são desativados.

Acesso ao menu de contexto e às janelas do aplicativo

Você pode usar o ícone para abrir o menu de contexto (na página 43) e a janela principal do aplicativo (consulte a seção "janela principal do Kaspersky Anti-Virus" na página 44).

- *Para abrir o menu de contexto,*

  role o ponteiro do mouse sobre o ícone e clique com o botão direito do mouse na área.

- *Para abrir a janela principal do aplicativo,*

  passe o cursor sobre o ícone e clique na área.

Se houver notícias da Kaspersky Lab disponíveis, o ícone será exibido na área de notificação da barra de tarefas do Microsoft Windows. Clique duas vezes nesse ícone para abrir a janela Agente de Notícias (consulte a seção "Agente de Notícias" na página 135).

MENU DE CONTEXTO

Você pode executar as tarefas de proteção básicas no menu de contexto.

O menu do Kaspersky Anti-Virus contém os seguintes itens:

- **Atualização** – executa a atualização dos bancos de dados e módulos do aplicativo.
- **Teclado Virtual** – exibe o Teclado Virtual.
- **Kaspersky Anti-Virus** – abre a janela principal do aplicativo.
- **Pausar a proteção/Reiniciar a proteção** – desativa/ativa temporariamente os componentes de proteção em tempo real. Esse item do menu não afeta as atualizações do aplicativo, nem a execução das verificações de vírus.
- **Configurações** – abre a janela de configurações do aplicativo.
- **Sobre** – abre uma janela com informações sobre o aplicativo.
- **Notícias** – abre a janela Agente de Notícias (consulte a seção "Agente de Notícias" na página 135). Este item de menu será exibido se houver notícias não lidas.

- Sair – fecha o Kaspersky Anti-Virus (ao selecionar esse item, o aplicativo é descartado da RAM do computador).

Figura 2. Menu de contexto

Se uma tarefa de verificação de vírus ou de atualização estiver em execução quando você abrir o menu de contexto, seu nome e o status de andamento (porcentagem concluída) serão exibidos no menu de contexto. Ao selecionar um item de menu com o nome de uma tarefa, você poderá alternar para a janela principal com um relatório dos resultados da execução da tarefa atual.

Para abrir o menu de contexto,

role o ponteiro do mouse sobre o ícone do aplicativo na área de notificação da barra de tarefas e clique com o botão direito do mouse.

Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

JANELA PRINCIPAL DO KASPERSKY ANTI-VIRUS

A janela principal do aplicativo contém os elementos de interface que dão acesso a todos os principais recursos do aplicativo.

A janela principal pode ser dividida em três partes:

- A parte superior da janela contém o indicador de status da proteção, que informa sobre o status atual da proteção do computador.

Figura 3. Status de proteção do computador atual

Existem três valores possíveis para o status de proteção: cada um deles é indicado por uma determinada cor. O verde indica que a proteção do computador está no nível correto; o amarelo e o vermelho indicam a existência de diversas ameaças de segurança. Além dos programas maliciosos, as ameaças incluem bancos de dados do aplicativo obsoletos, componentes de proteção desativados e a seleção de configurações mínimas de proteção.

As ameaças de segurança devem ser eliminadas assim que aparecem (consulte a seção "Diagnóstico e eliminação de problemas na proteção do computador" na página 51).

- À esquerda da janela, é possível alternar rapidamente para os principais recursos do aplicativo: ativar e desativar os componentes de proteção, executar tarefas de verificação de vírus, atualizar os bancos de dados e os módulos do programa, etc.

Figura 4. Parte esquerda da janela principal

- À direita da janela, existem informações sobre a função do aplicativo selecionada à esquerda, sendo possível definir suas configurações, fornecer ferramentas para a execução de tarefas de verificação de vírus, recuperar atualizações, etc.

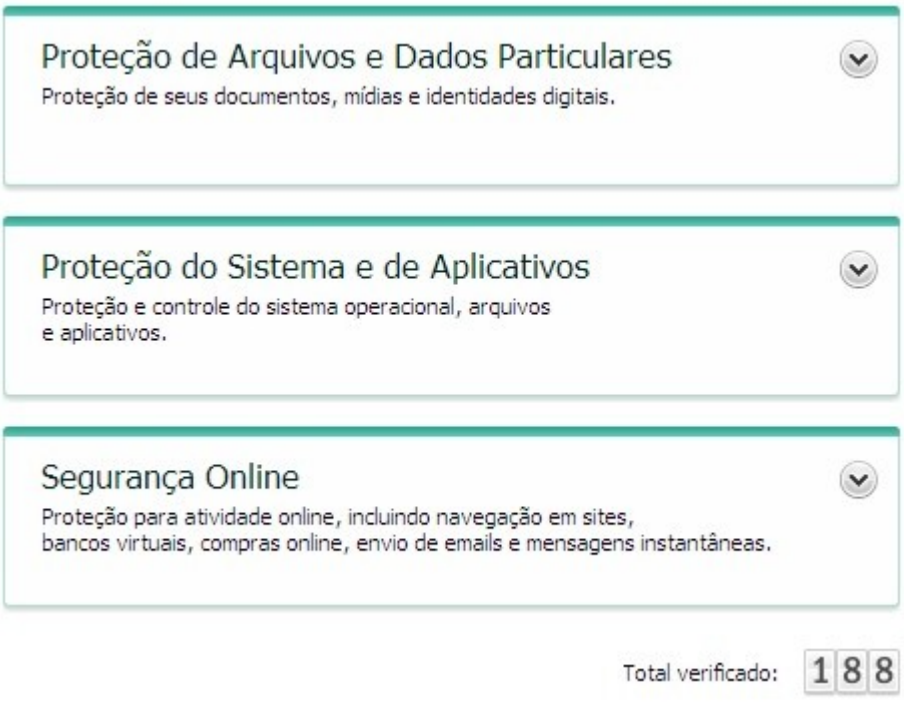

Proteção de Arquivos e Dados Particulares
Proteção de seus documentos, mídias e identidades digitais.
Proteção do Sistema e de Aplicativos
Proteção e controle do sistema operacional, arquivos e aplicativos.
Segurança Online
Proteção para atividade online, incluindo navegação em sites, bancos virtuais, compras online, envio de emails e mensagens instantâneas.
Total verificado: 188

Figura 5. Parte direita da janela principal

Você também pode usar os seguintes botões e links:

- Configurações – para abrir a janela de configurações do aplicativo.
- **Quarentena** – para trabalhar com objetos da Quarentena.
- **Relatórios** – alterna para o relatório de operação do aplicativo no formato de diagrama.

- **Notícias** – alterna para a exibição de notícias na janela Agente de Notícias (consulte a seção "Agente de Notícias" na página 135). Esse link será exibido depois que o aplicativo receber uma notícia.
- **Ajuda** – para exibir o sistema de Ajuda do Kaspersky Anti-Virus.
- **Minha Conta Kaspersky** – para entrar na conta pessoal do usuário no site do Serviço de Suporte Técnico (consulte a seção "Minha Conta Kaspersky" na página 143).
- **Suporte** – para abrir a janela com informações do sistema e links para os recursos de informações da Kaspersky Lab (site do Serviço de Suporte Técnico, fórum).
- **Licença** – ativação do Kaspersky Anti-Virus, renovação da licença.

Você pode alterar a aparência do Kaspersky Anti-Virus usando capas alternativas (consulte a seção "Aparência do aplicativo" na página 135).

Para abrir a janela principal do aplicativo:

- passe o cursor sobre o ícone do aplicativo na área de notificação da barra de tarefas e clique nele.

  Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

- selecione **Kaspersky Anti-Virus** no menu de contexto (consulte a seção "Menu de contexto" na página 43);
- clique no ícone do Kaspersky Anti-Virus na interface do Kaspersky Gadget (somente no Microsoft Windows Vista e no Microsoft Windows 7).

JANELAS DE NOTIFICAÇÃO E MENSAGENS POP-UP

O Kaspersky Anti-Virus notifica sobre eventos importantes que ocorrem durante sua operação, usando *janelas de notificação* e *mensagens pop-up* que são exibidas sobre o ícone do aplicativo na área de notificação da barra de tarefas.

As *janelas de notificação* são exibidas pelo Kaspersky Anti-Virus quando é possível executar diversas ações em relação a um evento: por exemplo, se um objeto malicioso for detectado, você poderá bloquear o acesso a ele, excluí-lo ou tentar desinfetá-lo. O aplicativo permite que você selecione uma das ações disponíveis. A janela de notificações desaparecerá da tela somente se você selecionar uma das ações.

Kaspersky Anti-Virus 2011
Ajuda
Verificação de vírus
Unidade removível conectada
É recomendável verificá-la quanto à presença de software malicioso
Deseja verificar a unidade removível?
Verificação Rápida
Apenas os arquivos possivelmente perigosos serão verificados
Verificação completa
Todos os arquivos na unidade removível serão verificados
Não verificar
A unidade removível não será verificada
Nesses casos, sempre executar

Figura 6. A janela Notificações

As *mensagens pop-up* são exibidas pelo Kaspersky Anti-Virus para informar sobre eventos que não exigem a seleção de uma ação. Algumas mensagens pop-up contêm links que podem ser usados para executar uma ação disponibilizada pelo aplicativo: por exemplo, executar a atualização dos bancos de dados ou iniciar a ativação do aplicativo). As mensagens pop-up desaparecem da tela automaticamente logo após sua exibição.

Figura 7. Mensagem pop-up

Dependendo do grau de importância do evento para a segurança do computador, você poderá receber os seguintes tipos de notificações:

- Notificações críticas – informa sobre os eventos de importância fundamental da perspectiva da segurança do computador: por exemplo, a detecção de um objeto malicioso ou de uma atividade perigosa no sistema. As janelas de notificação e mensagens pop-up desse tipo são vermelhas.

- Notificações importantes – informa sobre os eventos que possivelmente são importantes da perspectiva da segurança do computador: por exemplo, a detecção de um objeto possivelmente infectado ou de uma atividade suspeita no sistema. As janelas de notificação e mensagens pop-up desse tipo são amarelas.

- Notificações informativas – informam sobre eventos não críticos da perspectiva de segurança. As janelas de notificação e mensagens pop-up desse tipo são verdes.

JANELA DE CONFIGURAÇÃO DO APLICATIVO

A janela de configurações do Kaspersky Anti-Virus foi criada para configurar todo o aplicativo, componentes de proteção individuais, tarefas de verificação e atualização e para executar outras tarefas de configuração avançada (consulte a seção "Configurações avançadas do aplicativo" na página 75).

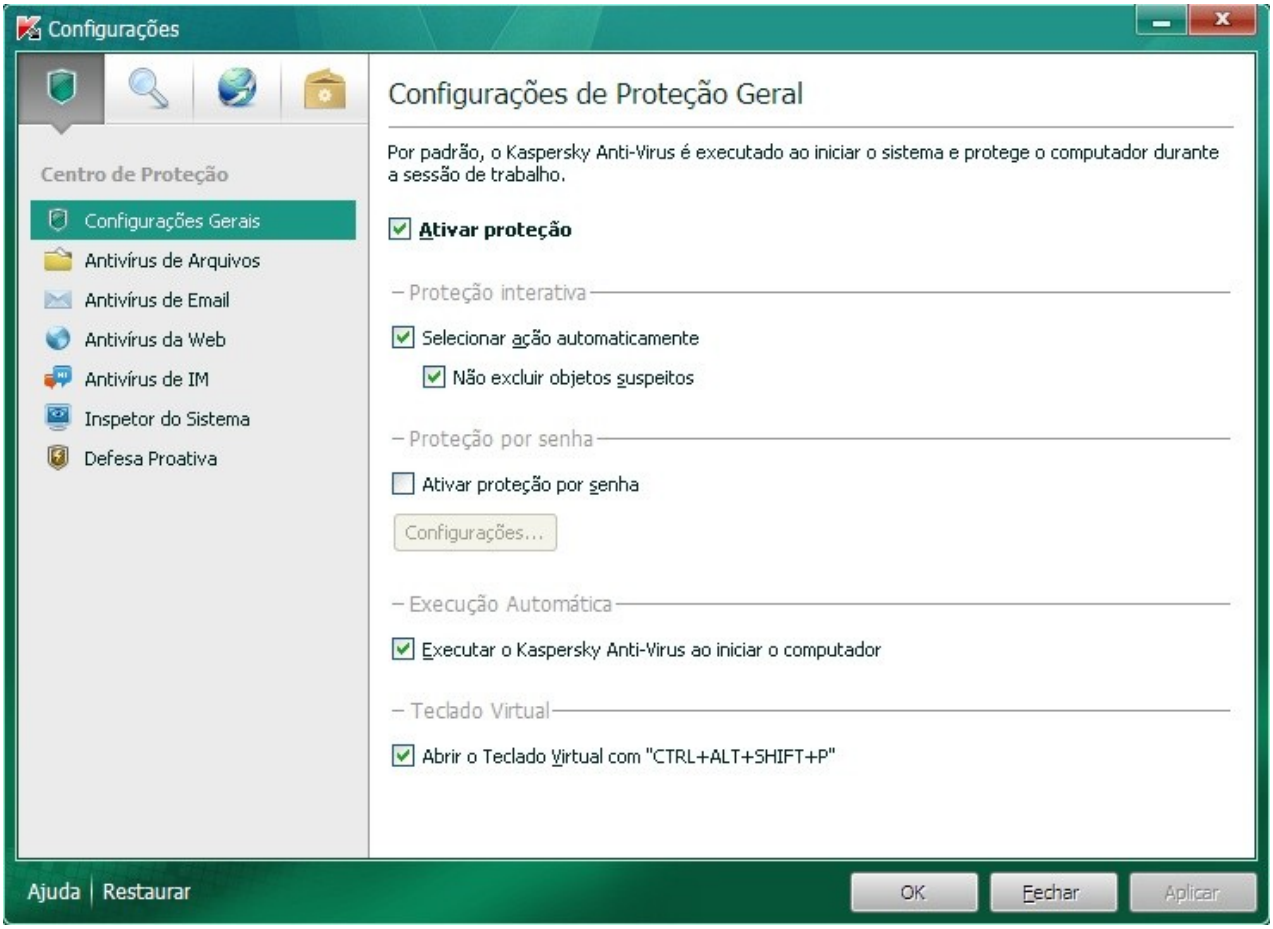


Figura 8. Janela de configuração do aplicativo

A janela de configurações do aplicativo consiste em duas partes:

- à esquerda da janela, você pode escolher o componente, a tarefa ou outro item do aplicativo para ser configurado;
- à direita da janela estão os controles que podem ser usados para configurar o item selecionado à esquerda.

Os componentes, as tarefas e outros itens à esquerda da janela estão organizados nas seguintes seções:

– **Centro de Proteção**;

– **Verificação**;

– **Centro de Atualizações**;

– **Configurações Avançadas**.

Para abrir a janela de configurações:

- clique no link **Configurações** na parte superior da janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44);
- selecione **Configurações** no menu de contexto (consulte a seção "Menu de contexto" na página 43);
- clique no botão com o ícone **Configurações** na interface do Kaspersky Gadget (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7). É necessário atribuir a opção para abrir a janela de configurações ao botão (consulte a seção "Como usar o Kaspersky Gadget" na página 73).

Para selecionar a janela desejada na janela de configurações,

clique no ícone correspondente à seção na parte superior esquerda da janela (veja a figura acima).

KASPERSKY GADGET

Ao usar o Kaspersky Anti-Virus em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você também pode usar o Kaspersky Gadget (aqui chamado de *gadget*).

O Kaspersky Gadget foi criado para acessar rapidamente os principais recursos do aplicativo: indicação de status da proteção, verificação de objetos quanto à presença de vírus, relatórios de operação do aplicativo, etc.

Depois de instalar o Kaspersky Anti-Virus em um computador com o Microsoft Windows 7, o gadget é exibido automaticamente na área de trabalho. Depois de instalar o aplicativo em um computador com o Microsoft Windows Vista, você deverá adicionar o gadget manualmente à Barra Lateral do Microsoft Windows (consulte a documentação do sistema operacional).

Figura 9. Kaspersky Gadget

INICIANDO E INTERROMPENDO O APLICATIVO

Depois que o Kaspersky Anti-Virus for instalado, ele será executado automaticamente. O aplicativo é executado automaticamente sempre que o sistema operacional é iniciado.

NESTA SEÇÃO:

Ativando e desativando a execução automática 50

Iniciando e interrompendo o aplicativo manualmente 50

ATIVANDO E DESATIVANDO A EXECUÇÃO AUTOMÁTICA

A execução automática do aplicativo indica que o Kaspersky Anti-Virus é iniciado após a inicialização do sistema operacional. Este é o modo de inicialização padrão.

- *Para ativar ou desativar a execução automática do aplicativo:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione a subseção **Configurações Gerais**.
  3. Para desativar a execução automática do aplicativo, desmarque a caixa **Executar o Kaspersky Anti-Virus ao iniciar o computador** na seção **Execução automática** à direita da janela. Marque esta caixa para ativar a execução automática do aplicativo.

INICIANDO E INTERROMPENDO O APLICATIVO MANUALMENTE

Os especialistas da Kaspersky Lab não recomendam interromper o Kaspersky Anti-Virus, pois a proteção do computador e de seus dados pessoais estará em risco. Se for realmente necessário desativar a proteção, é recomendável pausar a proteção do computador por um determinado período, sem sair do aplicativo.

O Kaspersky Anti-Virus deverá ser iniciado manualmente se você tiver desativado a execução automática do aplicativo (consulte a seção "Ativando e desativando a execução automática" na página 50).

- *Para executar o aplicativo manualmente,*

  no menu **Iniciar**, selecione **Programas** → **Kaspersky Anti-Virus 2011** → **Kaspersky Anti-Virus 2011**.

- *Para sair do aplicativo,*

  clique com o botão direito do mouse para abrir o menu de contexto do ícone do aplicativo na área de notificações da barra de tarefas e selecione **Sair**.

Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

STATUS DE PROTEÇÃO DO COMPUTADOR

Esta seção contém informações sobre como descobrir se o computador está protegido ou se sua segurança está ameaçada, além de como eliminar as ameaças emergentes. Também é possível encontrar informações sobre como ativar, desativar e pausar a proteção ao trabalhar com o Kaspersky Anti-Virus.

NESTA SEÇÃO:

Diagnóstico e eliminação de problemas na proteção do computador 51

Ativando e desativando a proteção 53

Pausando e reiniciando a proteção 54

DIAGNÓSTICO E ELIMINAÇÃO DE PROBLEMAS NA PROTEÇÃO DO COMPUTADOR

Os problemas com a proteção do computador são indicados por seu indicador de status localizado na parte superior da janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44). A cor do indicador muda de acordo com o status de proteção do host: o verde indica que o computador está protegido; o amarelo indica problemas relacionados com a proteção e o vermelho alerta sobre ameaças graves à segurança do computador. É recomendável corrigir os problemas e as ameaças de segurança imediatamente.

Ao clicar no ícone do indicador na janela principal do aplicativo, é aberta a janela **Status de proteção** (veja a figura a seguir), que contém informações detalhadas sobre o status da proteção do computador e sugestões para a solução dos problemas e ameaças detectadas.

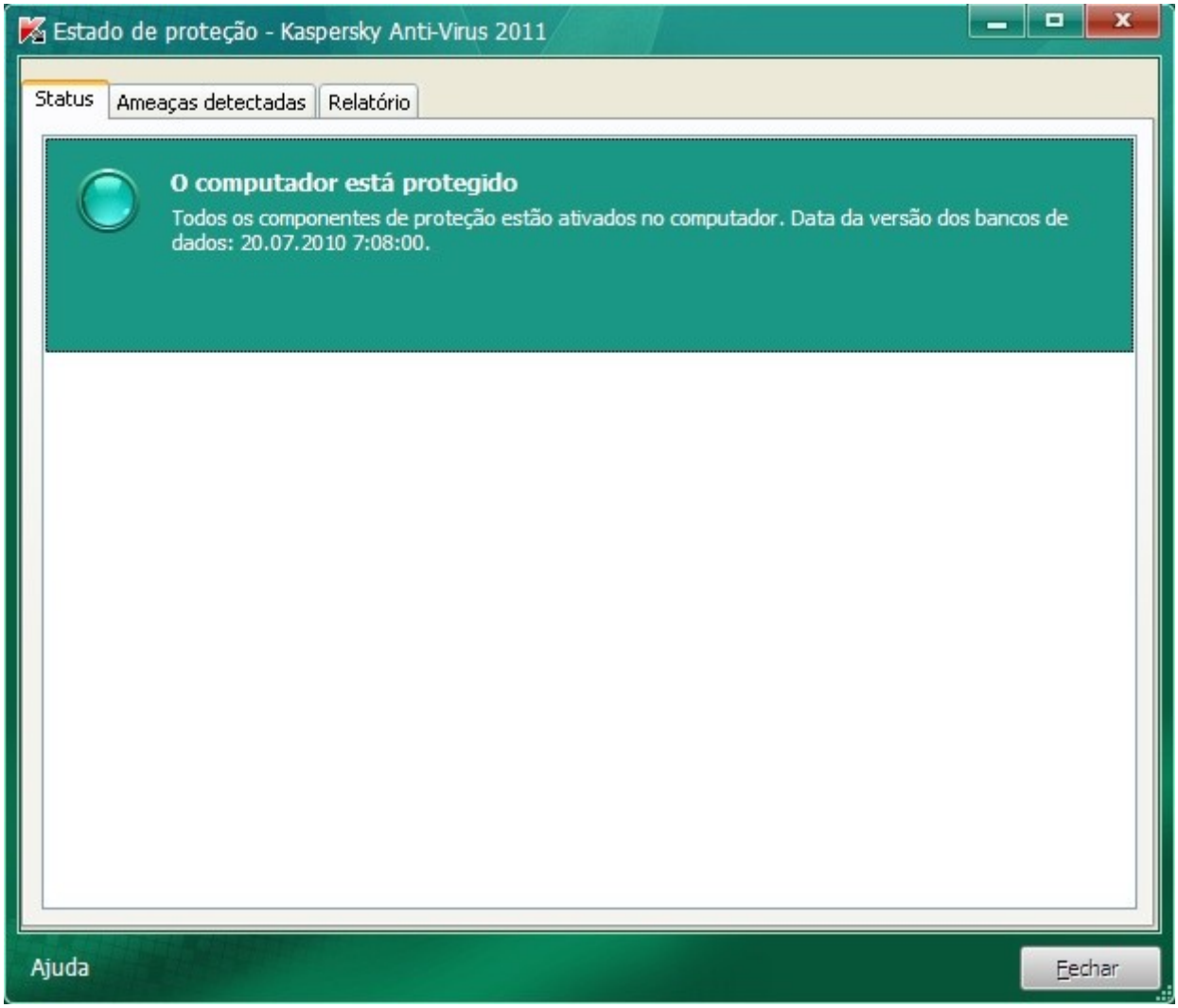

Estado de proteção - Kaspersky Anti-Virus 2011
Status
Ameaças detectadas
Relatório
O computador está protegido
Todos os componentes de proteção estão ativados no computador. Data da versão dos bancos de dados: 20.07.2010 7:08:00.
Ajuda
Fechar

Figura 10. Resolvendo problemas de segurança

A guia **Status** da janela **Estado de proteção** lista os problemas relacionados com a proteção, inclusive aqueles causados por desvios do modo de operação normal do produto (como bancos de dados desatualizados). Para tratar dos problemas, o produto oferece as seguintes opções de ação:

- Remover imediatamente. Clicar nos botões correspondentes o levará para a solução apropriada do problema. Essa é a ação recomendada.

- Adiar remoção. Se, por algum motivo, a remoção imediata do problema não for possível, você poderá adiar essa ação e voltar a ela mais tarde. Para fazê-lo, clique no botão **Ocultar mensagem**.

  No caso de problemas graves, o adiamento da remoção não estará disponível. Esses problemas incluem, por exemplo, objetos maliciosos que não foram desinfetados, interrupção de um ou de vários componentes ou corrupção dos arquivos do programa.

Para exibir na lista comum as notificações ocultas anteriormente, marque a caixa **Mostrar mensagens ocultas** que será exibida na parte inferior da guia quando houver mensagens ocultas.

Você pode usar a guia **Ameaças detectadas** para exibir a lista de malware e riskware descobertos e selecionar a ação que será executada com esses objetos (por exemplo, mover para a Quarentena). Para selecionar uma operação, use os controles acima da lista e o menu de contexto dos registros listados.

Na guia **Relatório**, é possível exibir os relatórios de atividade do aplicativo (consulte a seção "Onde exibir o relatório de operação do aplicativo" na página 69).

ATIVANDO E DESATIVANDO A PROTEÇÃO

Por padrão, o Kaspersky Anti-Virus é executado ao carregar o sistema operacional e protege o computador até que ele seja desligado. Todos os componentes de proteção são executados.

Você pode desativar a proteção fornecida pelo Kaspersky Anti-Virus total ou parcialmente.

Os especialistas da Kaspersky Lab recomendam enfaticamente que você não desative a proteção, pois isso pode levar à infecção do computador e à perda de dados. Se for realmente necessário, é recomendável pausar a proteção pelo período desejado (consulte a seção "Pausando e reiniciando a proteção" na página 54).

Quando a proteção é desativada, todos os seus componentes ficam inativos.

Isso é indicado da seguinte maneira:

- ícone do aplicativo inativo (cinza) na área de notificações da barra de tarefas (consulte a seção "Ícone da área de notificação" na ´página 42);
- indicador de segurança vermelho na parte superior da janela principal do aplicativo.

Nesse caso, a proteção é considerada no contexto dos componentes de proteção. Desativar ou pausar os componentes de proteção não afeta o desempenho das tarefas de verificação de vírus e das atualizações do Kaspersky Anti-Virus.

Você pode ativar ou desativar a proteção completamente na janela de configurações do aplicativo (consulte a seção "Janela de configurações do aplicativo" na página 48). você pode ativar ou desativar componentes individuais do aplicativo na janela de configurações ou na janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).

Para ativar ou desativar a proteção completamente:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, selecione a seção **Centro de Proteção**, subseção **Configurações Gerais**.
3. Desmarque a caixa **Ativar proteção** para desativar a proteção. Se desejar ativar a proteção, marque a caixa.

Para ativar ou desativar um componente de proteção na janela de configurações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente que deve ser ativado ou desativado.
3. À direita da janela, desmarque a caixa **Ativar <nome do componente>** para desativar esse componente. Se desejar ativar o componente, marque a caixa.

Para ativar ou desativar um componente de proteção na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Centro de Proteção**.
2. À direita da janela, clique na seção que contém o componente que deve ser ativado ou desativado.
3. Abra o menu de seleção de ações clicando no botão com o nome do componente. Selecione **Ativar <nome do componente>** para ativar esse componente ou selecione **Desativar <nome do componente>** para desativá-lo.

   Ao ativar um componente, o ícone à sua esquerda fica verde; ao desativá-lo, o ícone fica cinza.

PAUSANDO E REINICIANDO A PROTEÇÃO

Pausar a proteção significa desativar temporariamente todos os componentes de proteção por um determinado período.

Isso é indicado da seguinte maneira:

- ícone do aplicativo inativo (cinza) na área de notificações da barra de tarefas (consulte a seção "Ícone da área de notificação" na ´página 42);
- indicador de segurança vermelho na parte superior da janela principal do aplicativo.

Nesse caso, a proteção é considerada no contexto dos componentes de proteção. Desativar ou pausar os componentes de proteção não afeta o desempenho das tarefas de verificação de vírus e das atualizações do Kaspersky Anti-Virus.

Se foram estabelecidas conexões de rede enquanto a proteção estava pausada, será exibida uma notificação sobre a interrupção dessas conexões.

Ao trabalhar em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você pode pausar a proteção usando o Kaspersky Gadget. Para fazer isso, o Kaspersky Gadget deve estar configurado de forma que a opção de abrir a janela de relatórios seja atribuída a um de seus botões (consulte a seção "Como usar o Kaspersky Gadget" na página 73).

Para pausar a proteção do computador:

1. Abra a janela **Pausar a proteção** usando um dos seguintes métodos:
   - selecione **Pausar a proteção** no menu de contexto do ícone do aplicativo (consulte a seção "Menu de contexto" na página 43);
   - clique no botão com o ícone **Pausar a proteção** na interface do Kaspersky Gadget (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7).
2. Na janela **Pausar a proteção**, selecione o intervalo de tempo depois do qual a proteção deve ser reiniciada:
   - **Pausar pelo tempo especificado** – a proteção será ativada depois do intervalo de tempo especificado no campo abaixo.
   - **Pausar até reiniciar** – a proteção será ativada depois que o aplicativo ou o sistema operacional forem reiniciados (desde que a execução automática do aplicativo esteja ativada (consulte a seção "Ativando e desativando a execução automática" na página 50)).
   - **Pausar** – a proteção será ativada somente quando você decidir reiniciá-la (veja a seguir).

Para reiniciar a proteção do computador,

selecione **Reiniciar a proteção** no menu de contexto do ícone do aplicativo (consulte a seção "Menu de contexto" na página 43).

Você pode usar este método para reiniciar a proteção do computador quando a opção **Pausar** tiver sido selecionada ou quanto você tiver selecionado **Pausar pelo tempo especificado** ou **Pausar até reiniciar**.

SOLUCIONANDO TAREFAS TÍPICAS

Esta seção contém instruções para as tarefas básicas com as quais a maioria dos usuários se depara ao trabalhar com o aplicativo.

NESTA SEÇÃO:

Como ativar o aplicativo 55

Como comprar ou renovar a licença 56

O que fazer quando forem exibidas notificações do aplicativo 57

Como atualizar os bancos de dados e módulos do aplicativo 57

Como verificar as áreas críticas do computador quanto à presença de vírus 58

Como verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus 59

Como executar a verificação completa do computador quanto à presença de vírus 60

Verificando vulnerabilidades no computador 61

Como proteger seus dados pessoais contra roubo 61

O que fazer se você suspeitar que um objeto está infectado com um vírus 63

O que fazer se você suspeitar que o computador está infectado 64

Como restaurar um objeto excluído ou desinfetado pelo aplicativo 66

Como criar e usar o Disco de Recuperação 66

Como exibir o relatório de operação do aplicativo 69

Como restaurar as configurações padrão do aplicativo 69

Como importar as configurações do aplicativo Kaspersky Anti-Virus instalado em outro computador 70

Como alternar do Kaspersky Anti-Virus para o Kaspersky Internet Security 71

Como usar o Kaspersky Gadget 73

COMO ATIVAR O APLICATIVO

A *ativação* é o procedimento para ativar a licença que permite usar uma versão totalmente funcional do aplicativo até a expiração da licença.

Se você não ativou o aplicativo durante a instalação, pode fazer isso posteriormente. O Kaspersky Anti-Virus exibirá notificações na área de notificações da barra de tarefas sobre a necessidade de ativar o aplicativo.

➧ *Para executar o Assistente de Ativação do Kaspersky Anti-Virus:*

- Clique no link **Ative o aplicativo** na janela de notificações do Kaspersky Anti-Virus exibida na área de notificações da barra de tarefas.

- Clique no link **Licença** na parte inferior da janela principal do aplicativo. Na janela **Gerenciamento de licenças** que é aberta, clique no botão **Ativar o aplicativo com uma nova licença**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Step 1. Seleção do tipo de licença e inserção do código de ativação

Confirme se você selecionou **Ativar a versão comercial** na janela do Assistente de Ativação, insira o código de ativação (consulte a seção "Sobre o código de ativação" na página 40) no campo correspondente e clique no botão **Avançar**.

Step 2. Solicitando a ativação

Na primeira etapa, o Assistente envia uma solicitação ao servidor de ativação para obter a permissão para ativar a versão comercial do aplicativo. Se a solicitação for enviada com êxito, o Assistente continuará automaticamente na etapa seguinte.

Step 3. Inserção de dados de registro

O registro do usuário é necessário para que ele possa entrar em contato com o Serviço de Suporte. Os usuários não registrados recebem apenas um suporte mínimo.

Especifique seus dados de registro e clique no botão **Avançar**.

Step 4. Ativação

Nesta etapa, o Assistente se conecta ao servidor de ativação para concluir a ativação do aplicativo e o registro do usuário, após o qual o Assistente continuará automaticamente na janela seguinte.

Step 5. Conclusão do Assistente

Esta janela exibe informações sobre os resultados da ativação: o tipo de licença usado e a data de expiração da licença.

Clique no botão **Concluir** para fechar o assistente.

COMO COMPRAR OU RENOVAR A LICENÇA

Se você tiver instalado o Kaspersky Anti-Virus sem uma licença, poderá comprar uma após a instalação. Quando sua licença expirar, você poderá renová-la. Você receberá um código de ativação que deve ser usado para ativar o aplicativo (consulte a seção "Como ativar o aplicativo" na página 55).

Para comprar uma licença:

1. Abra a janela principal do aplicativo.
2. Clique no botão **Comprar licença** na parte inferior da janela.

   A página da loja virtual na Web na qual você pode comprar uma licença é aberta.

Para renovar uma licença:

1. Abra a janela principal do aplicativo e clique no link **Licença** na parte inferior da janela.

   A janela **Gerenciamento de licenças** é aberta.
2. Clique no botão **Renovar licença**.

A página do centro de renovação de licenças na Web na qual você pode renovar sua licença é aberta.

O QUE FAZER QUANDO FOREM EXIBIDAS NOTIFICAÇÕES DO APLICATIVO

As notificações que são exibidas na área de notificação da barra de tarefas informam sobre eventos que ocorrem durante a operação do aplicativo e que requerem sua atenção. Dependendo do grau de importância do evento, você poderá receber os seguintes tipos de notificações:

- Notificações críticas – informa sobre os eventos de importância fundamental da perspectiva da segurança do computador: por exemplo, a detecção de um objeto malicioso ou de uma atividade perigosa no sistema. As janelas de notificação e mensagens pop-up desse tipo são vermelhas.
- Notificações importantes – informa sobre os eventos que possivelmente são importantes da perspectiva da segurança do computador: por exemplo, a detecção de um objeto possivelmente infectado ou de uma atividade suspeita no sistema. As janelas de notificação e mensagens pop-up desse tipo são amarelas.
- Notificações informativas – informam sobre eventos não críticos da perspectiva de segurança. As janelas de notificação e mensagens pop-up desse tipo são verdes.

Se alguma dessas notificações forem exibidas na tela, selecione uma das opções sugeridas. Por padrão, a opção ideal é aquela recomendada pelos especialistas da Kaspersky Lab.

COMO ATUALIZAR OS BANCOS DE DADOS E MÓDULOS DO APLICATIVO

Por padrão, o Kaspersky Anti-Virus verifica automaticamente as atualizações nos servidores de atualização da Kaspersky Lab. Se o servidor contiver novas atualizações, o Kaspersky Anti-Virus as baixará e instalará em background. Você pode iniciar a atualização do Kaspersky Anti-Virus a qualquer momento.

Para baixar atualizações dos servidores da Kaspersky Lab, é necessário estabelecer uma conexão com a Internet.

Para iniciar a atualização no menu de contexto,

selecione **Atualização** no menu de contexto do ícone do aplicativo.

Para iniciar a verificação na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Centro de Atualizações** à esquerda da janela.
2. Clique no botão **Executar Atualização** à direita da janela.

   São exibidas informações sobre a atualização em andamento:

   - na seção **Atualização** da janela principal do aplicativo, na subseção **Atualização em andamento** ;
   - na janela **Atualização** que é aberta ao clicar no botão **Atualização em andamento**;
   - no menu de contexto do ícone do aplicativo.

Para interromper a atualização:

1. Abra a janela principal do aplicativo e selecione a seção **Centro de Atualizações** à esquerda da janela.
2. Clique no botão **Atualização em andamento** à direita da janela.

3. Na janela **Atualização** que é aberta, clique no botão **Interromper**.

4. Na janela que solicita a confirmação do usuário, clique no botão **Sim**.

COMO VERIFICAR AS ÁREAS CRÍTICAS DO COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

A verificação das áreas críticas consiste em verificar os objetos que são carregados na inicialização do sistema operacional, verificar a memória do sistema, os setores de inicialização da unidade de disco e os objetos que foram adicionados pelo usuário (consulte a seção "Criando uma lista de objetos a serem verificados" na página 80).

Você pode executar a verificação de áreas críticas usando um dos métodos a seguir:

- usando o atalho criado anteriormente (veja a página 84);
- na janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).

Para iniciar a verificação usando um atalho:

1. Abra a janela do Microsoft Windows Explorer e vá para a pasta na qual você criou o atalho.
2. Clique duas vezes no atalho para iniciar a verificação.

   São exibidas informações sobre a verificação em andamento:

   - na seção **Verificação** da janela principal do aplicativo, na seção **Verificação das Áreas Críticas em andamento**;
   - na seção **Verificação de Áreas Críticas** que é aberta clicando no botão **Verificação das Áreas Críticas em andamento**;
   - no menu de contexto do ícone do aplicativo.

Para iniciar a verificação na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** à esquerda da janela.
2. À direita da janela principal do aplicativo, clique no botão **Executar Verificação das Áreas Críticas**.

   São exibidas informações sobre a verificação em andamento:

   - na seção **Verificação** da janela principal do aplicativo, na seção **Verificação das Áreas Críticas em andamento**;
   - na seção **Verificação de Áreas Críticas** que é aberta clicando no botão **Verificação das Áreas Críticas em andamento**;
   - no menu de contexto do ícone do aplicativo.

Para interromper a verificação das áreas críticas:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** à esquerda da janela.
2. À direita da janela, clique no botão **Verificação das Áreas Críticas em andamento**.
3. Na janela **Verificação de Áreas Críticas** que é aberta, clique no botão **Interromper**.
4. Na janela que solicita a confirmação do usuário, clique no botão **Sim**.

COMO VERIFICAR UM ARQUIVO, PASTA, DISCO OU OUTRO OBJETO QUANTO À PRESENÇA DE VÍRUS

Você pode usar os seguintes métodos para verificar um objeto quanto à presença de vírus:

- usando o menu de contexto do objeto;
- na janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44);
- usando o gadget do Kaspersky Anti-Virus (apenas no Microsoft Windows Vista e no Microsoft Windows 7).

Para iniciar a tarefa de verificação de vírus no menu de contexto do objeto:

1. Abra a janela do Microsoft Windows Explorer e vá para a pasta que contém o objeto que deve ser verificado.
2. Clique com o botão direito do mouse no menu de contexto do objeto (veja a figura a seguir) e selecione **Verificar Vírus**.

   O processo e os resultados da tarefa serão exibidos na janela **Verificação de Vírus** que é aberta.

Figura 11. Menu de contexto de um objeto no Microsoft Windows

Para iniciar a verificação de um objeto na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** à esquerda da janela.
2. Especifique o objeto que deve ser verificado usando um dos seguintes métodos:
   - Clique no link **selecionar** à direita da janela para abrir a janela **Verificação Personalizada** e marque as caixas ao lado das pastas e unidades que você deseja verificar. Se a janela não exibir nenhum objeto a ser verificado, abra a janela **Selecionar objeto a ser verificado** clicando no link **Adicionar** e selecione os objetos que devem ser verificados.
   - Arraste um objeto a ser verificado para a área exclusiva da janela principal (veja a figura a seguir).

O andamento da tarefa é exibido na janela **Verificação de Vírus** que é aberta.

Figura 12. Área da janela para a qual você deve arrastar um objeto a ser verificado

- *Para verificar um objeto quanto à presença de vírus usando o gadget,*

  arraste o objeto a ser verificado para o gadget.

  O andamento da tarefa é exibido na janela **Verificação de Vírus** que é aberta.

- *Para interromper a verificação de objetos:*

  1. Na janela **Verificação de Vírus** que é aberta depois que a verificação de objetos é iniciada, clique no botão **Interromper** ou feche a janela.
  2. Na janela Verificação de Vírus que é aberta solicitando que o usuário confirme a interrupção da verificação, clique no botão **Sim**.

COMO EXECUTAR A VERIFICAÇÃO COMPLETA DO COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

Você pode executar a verificação completa de vírus usando um dos seguintes métodos:

- usando o atalho criado anteriormente (veja a página 84);
- na janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).

- *Para iniciar a verificação completa usando um atalho:*

  1. Abra a janela do Microsoft Windows Explorer e vá para a pasta na qual você criou o atalho.
  2. Clique duas vezes no atalho para iniciar a verificação.

     São exibidas informações sobre a verificação em andamento:

     - na seção **Verificação** da janela principal do aplicativo, na seção **Verificação Completa em andamento**;
     - na janela **Verificação Completa** que é aberta clicando na seção **Verificação Completa em andamento**;
     - no menu de contexto do ícone do aplicativo.

- *Para iniciar a verificação completa na janela principal do aplicativo:*

  1. Abra a janela principal do aplicativo e selecione a seção **Verificação** à esquerda da janela.
  2. À direita da janela, clique no botão **Executar Verificação Completa**.

     São exibidas informações sobre a verificação em andamento:

     - na seção **Verificação** da janela principal do aplicativo, na seção **Verificação Completa em andamento**;

- na janela **Verificação Completa** que é aberta clicando na seção **Verificação Completa em andamento**;
- no menu de contexto do ícone do aplicativo.

Para interromper a verificação completa:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** à esquerda.
2. À direita da janela, clique no botão **Verificação Completa em andamento**.
3. Na janela **Verificação Completa** que é aberta, clique no botão **Interromper**.
4. Na janela que solicita a confirmação do usuário, clique no botão **Sim**.

VERIFICANDO VULNERABILIDADES NO COMPUTADOR

Vulnerabilidades são partes não protegidas do código do software que os invasores podem usar deliberadamente para atingir seus objetivos, como copiar os dados usados em aplicativos não protegidos. A verificação de vulnerabilidades no computador ajuda a descobrir esses pontos fracos. É recomendável remover as vulnerabilidades detectadas.

Você pode usar os seguintes métodos para verificar vulnerabilidades no sistema:

- na janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44);
- usando o atalho criado anteriormente.

Para iniciar a tarefa usando um atalho:

1. Abra o Microsoft Windows Explorer e vá para a pasta na qual você criou o atalho.
2. Clique duas vezes no atalho para executar a verificação de vulnerabilidades no sistema.

   O andamento da tarefa será exibido na janela **Verificação de Vulnerabilidades** que é aberta.

Para iniciar a tarefa na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** à esquerda da janela.
2. Clique no botão **Verificação de Vulnerabilidades** à direita da janela.

   O andamento da tarefa será exibido na janela **Verificação de Vulnerabilidades** que é aberta.

Para interromper a verificação de vulnerabilidades:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** à esquerda da janela.
2. Clique no botão **Verificação de Vulnerabilidades** à direita da janela.
3. Na janela **Verificação de Vulnerabilidades** que é aberta, clique no botão **Interromper**.
4. Na janela que solicita a confirmação do usuário para interromper a verificação, clique no botão **Sim**.

COMO PROTEGER SEUS DADOS PESSOAIS CONTRA ROUBO

Com o Kaspersky Anti-Virus, Você pode proteger seus dados pessoais contra roubo, incluindo:

- senhas, nomes de usuário e outros dados de registro;

- números de contas e cartões bancários.

O Kaspersky Anti-Virus inclui componentes e ferramentas que permitem proteger seus dados pessoais contra tentativas de roubo feitas por hackers usando métodos como phishing e interceptação de dados digitados no teclado.

A proteção contra phishing é garantida pelo Antiphishing implementado nos componentes Antivírus da Web e Antivírus de IM.

A proteção contra a interceptação de dados digitados no teclado é assegurada com o uso do *Teclado Virtual*.

NESTA SEÇÃO:

Proteção contra phishing 62

Teclado Virtual 62

PROTEÇÃO CONTRA PHISHING

Phishing é um tipo de fraude online que consiste em enganar os usuários para que divulguem seus números de cartão de crédito, códigos PIN e outros detalhes pessoais, com o objetivo de roubar quantias em dinheiro.

Frequentemente, o phishing é direcionado aos usuários de bancos virtuais. Os criminosos criam uma cópia exata do site de um banco escolhido e enviam emails aos clientes em nome do banco. Nesses emails, eles alegam que um erro ou uma substituição no software do sistema do banco virtual resultou na perda de informações dos usuários, sendo necessário que o usuário as confirme ou modifique no site do banco. Os usuários clicam no link que os leva ao site falso, inserem suas informações que terminam então nas mãos dos criminosos.

A proteção contra phishing é garantida pelo Antiphishing implementado nos componentes Antivírus da Web e Antivírus de IM. Ative esses componentes para garantir a proteção abrangente contra phishing.

Para ativar os componentes que oferecem proteção contra phishing:

1. Abra a janela principal do aplicativo e selecione a seção **Centro de Proteção** à esquerda da janela.
2. À direita da janela, clique para abrir a seção **Segurança Online**.
3. Abra o menu para selecionar uma ação do componente clicando no botão **Antiphishing** e selecionando **Ativar Antiphishing** no menu.

   Essa ação ativa o Antiphishing e todos os componentes do qual ele faz parte.

TECLADO VIRTUAL

Ao trabalhar no computador, em algumas situações, é necessário inserir seus dados pessoais, ou seu nome de usuário e sua senha. Isso acontece, por exemplo, ao registrar uma conta em sites, fazer compras online ou usar um banco virtual.

Existe um risco de que essas informações pessoais sejam interceptadas usando interceptadores de teclado ou keyloggers, que são programas que registram o pressionamento de teclas.

A ferramenta Teclado Virtual evita a interceptação dos dados inseridos usando o teclado.

O Teclado Virtual não poderá proteger seus dados pessoais se o site que exibe a inserção desses dados tiver sido invadido; nesse caso, as informações são obtidas diretamente pelos invasores.

Vários aplicativos classificados como spyware fazem capturas de tela que são transferidas para o invasor para análise e para roubar os dados pessoais do usuário. O Teclado Virtual evita que dados pessoais inseridos sejam interceptados por meio de capturas de tela.

O Teclado Virtual evita apenas a interceptação de dados de privacidade ao trabalhar com os navegadores Microsoft Internet Explorer e Mozilla Firefox.

Antes de começar a usar o Teclado Virtual, conheça suas características:

- Antes de inserir dados no Teclado Virtual usando o cursor, certifique-se de que o campo de entrada apropriado esteja selecionado.
- Você pode clicar nos botões do Teclado Virtual usando o mouse.
- Diferentemente dos teclados reais, no Teclado Virtual não é possível pressionar duas teclas simultaneamente. Portanto, para usar combinações de teclas (por exemplo, **ALT+F4**), clique na primeira tecla (por exemplo, **ALT**) e depois na próxima tecla (por exemplo **F4**); em seguida, clique na primeira tecla novamente. O segundo clique na tecla funciona da mesma forma que a liberação da mesma em um teclado real.
- O idioma de entrada do Teclado Virtual é alternado usando as combinações de teclas **CTRL+SHIFT** (a tecla **SHIFT** deve ser clicada usando o botão direito do mouse) ou **CTRL+LEFT ALT** (a tecla **LEFT ALT** deve ser clicada usando o botão direito do mouse) de acordo com as configurações especificadas.

Você pode abrir o Teclado Virtual das seguintes formas:

- no menu de contexto do ícone do aplicativo;
- nas janelas do navegador Microsoft Internet Explorer ou Mozilla Firefox;
- usando os atalhos de teclado.

Para abrir o Teclado Virtual no menu de contexto do ícone do aplicativo,

selecione o item **Teclado Virtual** no menu de contexto do ícone do aplicativo.

Para abrir o Teclado Virtual na janela do navegador,

clique no botão **Teclado Virtual** na barra de ferramentas do Microsoft Internet Explorer ou do Mozilla Firefox.

Para abrir o Teclado Virtual usando o teclado do computador,

use a seguintes combinação de teclas: **CTRL+ALT+SHIFT+P**.

O QUE FAZER SE VOCÊ SUSPEITAR QUE UM OBJETO ESTÁ INFECTADO COM UM VÍRUS

Se você suspeitar que um objeto está infectado, primeiro verifique-o usando o Kaspersky Anti-Virus (consulte a seção "Como verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus" na página 59).

Se, depois da verificação, o aplicativo relatar que o objeto não está infectado, apesar de você achar que sim, você poderá:

- Mover o objeto para a *Quarentena.* Os objetos movidos para a Quarentena não representam uma ameaça ao computador. Depois que os bancos de dados são atualizados, é provável que o Kaspersky Anti-Virus possa identificar a ameaça com certeza e eliminá-la.

- Enviar o objeto para o *Laboratório de Vírus*. Os especialistas do Laboratório de Vírus verificam o objeto. Se ele estiver infectado com um vírus, será imediatamente adicionado à descrição dos novos vírus nos bancos de dados que serão baixados pelo aplicativo com uma atualização (consulte a seção "Como atualizar os bancos de dados e módulos do aplicativo" na página 57).

Você pode mover um objeto para a Quarentena usando um dos métodos a seguir:

- usando o link **Mover para a Quarentena** na janela **Estado de proteção**;
- usando o menu de contexto do objeto.

Para mover um objeto para a Quarentena na janela Estado de proteção:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela principal para abrir a janela **Estado de proteção** na guia **Ameaças detectadas**.
3. Clique no botão **Mover para a Quarentena**.
4. Na janela que é aberta, selecione o objeto que você deseja mover para a Quarentena.

Para mover um objeto para a Quarentena usando o menu de contexto:

1. Abra o Microsoft Windows Explorer e vá para a pasta que contém o objeto que você deseja mover para a Quarentena.
2. Clique com o botão direito do mouse no menu de contexto do objeto e selecione **Mover para a Quarentena**.

Para enviar um objeto para o Laboratório de Vírus:

1. Vá para a página de solicitação do Laboratório de Vírus (http://support.kaspersky.com/virlab/helpdesk.html).
2. Siga as instruções na página para enviar sua solicitação.

O QUE FAZER SE VOCÊ SUSPEITAR QUE O COMPUTADOR ESTÁ INFECTADO

Se você suspeitar que o computador foi infectado, use o *Assistente de Restauração do Sistema* para neutralizar as consequências da atividade maliciosa no sistema. A Kaspersky Lab recomenda executar o Assistente depois de desinfetar o computador para assegurar que todas as ameaças e os danos causados pelas infecções tenham sido corrigidos.

O Assistente verifica se houve alterações no sistema, como: o acesso à rede foi bloqueado, as extensões de arquivos de formatos conhecidos foram alteradas, a barra de ferramentas foi bloqueada, etc. Esses danos podem ter várias causas. Eles podem incluir atividade de programas maliciosos, a configuração incorreta do sistema, falhas do sistema ou até mesmo a operação incorreta de aplicativos de otimização do sistema.

Depois de concluir a análise, o Assistente examina as informações a fim de avaliar se houve danos no sistema que exigem atenção imediata. Dependendo da análise, será gerada uma lista de ações necessárias para eliminar os problemas. O Assistente agrupa essas ações em categorias de acordo com a gravidade dos problemas detectados.

O Assistente consiste em uma série de telas (etapas) nas quais você navega usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Para iniciar o Assistente de Restauração do Sistema:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** à esquerda da janela.
2. À direita da janela, clique no botão **Restauração do Sistema**.

As etapas detalhadas do Assistente.

Step 1. Iniciando a restauração do sistema

Confirme se a opção do Assistente para **Pesquisar problemas causados por atividade de malware** está selecionada e clique no botão **Avançar**.

Step 2. Pesquisa de problemas

O Assistente procurará problemas e danos que devem ser corrigidos. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 3. Selecionando as ações de solução de problemas

Todos os problemas encontrados na etapa anterior são agrupados de acordo com o tipo de perigo que representam. Para cada grupo de problemas, a Kaspersky Lab recomenda uma sequência de ações para reparar os danos. Há três grupos de ações:

- *Ações altamente recomendadas* eliminam os problemas que representam uma ameaça de segurança grave. É recomendável executar todas as ações desse grupo.
- *Ações recomendadas* eliminam os problemas que representam uma possível ameaça. Também é recomendável executar todas as ações desse grupo.
- *Ações adicionais* reparam danos ao sistema que não representam uma ameaça atual, mas que podem colocar a segurança do computador em perigo no futuro.

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

É altamente recomendável não desmarcar as caixas selecionadas por padrão, pois isso pode deixar o computador vulnerável a ameaças.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Step 4. Eliminação de problemas

O Assistente executará as ações selecionadas na etapa anterior. A eliminação de problemas pode levar algum tempo. Quando a solução de problemas for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 5. Conclusão do Assistente

Clique no botão **Concluir** para fechar o assistente.

COMO RESTAURAR UM OBJETO EXCLUÍDO OU DESINFETADO PELO APLICATIVO

A Kaspersky Lab recomenda que você evite restaurar objetos excluídos e desinfetados, pois eles podem ser uma ameaça ao computador.

Se desejar restaurar um arquivo excluído ou desinfetado, poderá usar uma cópia de backup do mesmo que foi criada pelo aplicativo ao verificar o objeto.

Para restaurar um objeto que foi excluído ou desinfetado pelo aplicativo:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela principal para abrir a janela **Estado de proteção** na guia **Ameaças detectadas**.
3. Na lista suspensa localizada acima da lista de ameaças, selecione **Neutralizado**.

   A lista de objetos desinfetados e excluídos é exibida na guia **Ameaças detectadas**. Os objetos são agrupados de acordo com seus status. Para exibir as objetos em um grupo, clique no ícone **+** à esquerda do cabeçalho do grupo.
4. Clique com o botão direito do mouse no menu de contexto do objeto que deseja restaurar e selecione **Restaurar**.

COMO CRIAR E USAR O DISCO DE RECUPERAÇÃO

Depois instalar e configurar o Kaspersky Anti-Virus, verificar o computador e ter certeza de que ele não está infectado, é recomendável criar o Disco de Recuperação. Você poderá usar o Disco de Recuperação para verificar e desinfetar computadores infectados que não podem ser desinfetados usando outros métodos (por exemplo, com aplicativos antivírus).

NESTA SEÇÃO:

Criando o Disco de Recuperação 66

Inicializando o computador com o Disco de Recuperação 68

CRIANDO O DISCO DE RECUPERAÇÃO

Criar o Disco de Recuperação significa criar uma imagem de disco (arquivo ISO) com arquivos de configuração e bancos de dados de antivírus atualizados.

A imagem do disco de origem que serve como base para a criação do novo arquivo pode ser baixada do servidor da Kaspersky Lab ou copiada de uma fonte local.

Você pode criar o Disco de Recuperação usando o *Assistente para Criação do Disco de Recuperação*. O arquivo rescuecd.iso criado pelo Assistente é salvo no disco rígido do computador:

- no Microsoft Windows XP – na seguinte pasta: Documents and Settings\All Users\Dados de Aplicativos\Kaspersky Lab\AVP11\Data\Rdisk\;
- nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7 – na seguinte pasta: ProgramData\Kaspersky Lab\AVP11\Data\Rdisk\.

O Assistente consiste em uma série de telas (etapas) nas quais você navega usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Para iniciar o Assistente para Criação do Disco de Recuperação:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** à esquerda da janela.
2. À direita da janela, clique no botão **Disco de Recuperação**.

As etapas detalhadas do Assistente.

Step 1. Iniciando o Assistente. Pesquisando uma imagem de disco existente

A primeira janela do Assistente contém informações sobre o Disco de Recuperação que será criado.

Se o Assistente detectar um arquivo ISO do Disco de Recuperação existente na pasta exclusiva (veja acima), a caixa **Usar imagem ISO existente** será exibida na primeira janela do Assistente. Marque a caixa para usar o arquivo detectado como imagem ISO original e vá diretamente para a etapa **Atualizando imagem do disco** (veja a seguir). Desmarque a caixa se não quiser usar a imagem de disco encontrada, e o Assistente continuará na janela **Selecionar origem da imagem do disco**.

Step 2. Selecionar origem da imagem do disco

Se você marcou a caixa **Usar imagem ISO existente** na primeira janela do Assistente, esta etapa será ignorada.

Nesta etapa, você deve selecionar a origem do arquivo da imagem na lista de opções:

- Selecione **Copiar a imagem ISO da unidade local ou de rede** se você já tem um Disco de Recuperação ou uma imagem preparada para ele armazenada no computador ou em um recurso de rede local.
- Selecione a opção **Baixar a imagem ISO do servidor da Kaspersky Lab** se você não tem um arquivo de imagem e desejar baixá-lo do servidor da Kaspersky Lab (o tamanho do arquivo é aproximadamente 100 MB).

Step 3. Copiando (baixando) a imagem do disco

Se você marcou a caixa **Usar imagem ISO existente** na primeira janela do Assistente, esta etapa será ignorada.

Se na etapa anterior você selecionou a opção de copiar a imagem de uma fonte local (**Copiar a imagem ISO da unidade local ou de rede**), nesta etapa você deve especificar o caminho do arquivo ISO. Para fazer isso, clique no botão **Procurar**. Depois de especificar o caminho do arquivo, clique no botão **Avançar**. O andamento da cópia da imagem de disco será exibido na janela do Assistente.

Se você selecionou **Baixar a imagem ISO do servidor da Kaspersky Lab**, o andamento do download da imagem de disco será exibido imediatamente.

Quando a cópia ou o download da imagem ISO for concluído, o Assistente passará automaticamente para a etapa seguinte.

Step 4. Atualizando o arquivo da imagem

O procedimento de atualização do arquivo inclui:

- atualização dos bancos de dados de antivírus;

- atualização dos arquivos de configuração.

Os arquivos de configuração determinam a possibilidade de inicializar o computador a partir de um disco removível ou um CD/DVD gravado usando uma imagem do disco de recuperação fornecida pelo Assistente.

Ao atualizar os bancos de dados de antivírus, são usados aqueles distribuídos na última atualização do Kaspersky Anti-Virus. Se os bancos de dados estiverem obsoletos, é recomendável atualizar e reiniciar Assistente para Criação do Disco de Recuperação.

Para iniciar a atualização do arquivo ISO, clique no botão **Avançar**. O andamento da atualização será exibido na janela do Assistente.

Step 5. Gravando a imagem em uma mídia de dados

Nesta janela, o Assistente informa sobre a criação bem-sucedida do Disco de Recuperação e disponibiliza a gravação em uma mídia de dados.

Especifique uma mídia de dados para gravar a imagem ISO:

- Selecione **Gravar em CD/DVD** para gravar a imagem em um CD/DVD.

  Será solicitado que você especifique o CD/DVD no qual a imagem deve ser gravada. Em seguida, a imagem ISO será gravada nesse CD/DVD. O processo de gravação pode levar algum tempo; aguarde até que ele seja concluído.

- Selecione a opção **Gravar na unidade flash USB** para gravar a imagem em uma unidade removível.

  A Kaspersky Lab recomenda não gravar a imagem ISO em dispositivos que não foram criados especificamente para armazenamento de dados, como smartphones, celulares, PDAs e MP3 players. A gravação de imagens ISO nesses dispositivos pode causar seu funcionamento incorreto no futuro.

  Será solicitado que você especifique a unidade removível na qual a imagem deve ser gravada. Em seguida, a imagem ISO será gravada nessa unidade removível. O processo de gravação pode levar algum tempo; aguarde até que ele seja concluído.

- Selecione **Salvar a imagem do disco em arquivo na unidade local ou de rede** para gravar a imagem ISO no disco rígido instalado no computador ou em outro disco rígido que possa ser acessado pela rede.

  Você poderá especificar a pasta na qual a imagem deve ser gravada e o nome do arquivo ISO; em seguida, ele será gravado no disco rígido. O processo de gravação pode levar algum tempo; aguarde até que ele seja concluído.

Step 6. Conclusão do Assistente

Para concluir o Assistente, clique no botão **Concluir**. Você pode usar o disco criado para inicializar o computador (veja a página 68).

INICIALIZANDO O COMPUTADOR COM O DISCO DE RECUPERAÇÃO

Se não for possível iniciar o sistema operacional devido a um ataque de vírus, use o Disco de Recuperação.

Para iniciar o sistema operacional, você deve usar um CD/DVD ou uma unidade removível com o arquivo de imagem (.iso) do disco de recuperação gravado (consulte a seção "Criando o Disco de Recuperação" na página 66).

Nem sempre é possível carregar o computador a partir de uma unidade removível. Especificamente, não há suporte para esse modo em alguns modelos de computador obsoletos. Antes de desligar o computador para reiniciar a partir de uma unidade removível, verifique se a operação pode ser executada.

Para inicializar o computador com o Disco de Recuperação:

1. Nas configurações do BIOS, ative a inicialização a partir do CD/DVD ou da unidade removível (para obter informações detalhadas, consulte a documentação da placa mãe do computador).

2. Insira o CD/DVD com a imagem do Disco de Recuperação na unidade de CD/DVD do computador infectado ou conecte a unidade removível.

3. Reinicie o computador.

Para obter informações detalhadas sobre o uso do Disco de Recuperação, consulte o Manual do Usuário do Disco de Recuperação da Kaspersky.

COMO EXIBIR O RELATÓRIO DE OPERAÇÃO DO APLICATIVO

O Kaspersky Anti-Virus cria relatórios de operação para cada componente. No relatório, você pode descobrir, por exemplo, quantos objetos maliciosos (como vírus e cavalos de Troia) foram detectados e removidos pelo aplicativo durante o período especificado, quantas vezes o aplicativo foi atualizado nesse período, quantas mensagens de spam foram detectadas, além de várias outras informações.

Ao trabalhar em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você pode abrir relatórios usando o Kaspersky Gadget. Para fazer isso, o Kaspersky Gadget deve estar configurado de forma que a opção de abrir a janela de relatórios seja atribuída a um de seus botões (consulte a seção "Como usar o Kaspersky Gadget" na página 73).

Para exibir o relatório de operação do aplicativo:

1. Abra a janela **Estado de proteção** na guia **Relatório** usando um dos seguintes métodos:

   - clique no botão **Relatórios** na parte superior da janela principal do aplicativo;

   - clique no botão com o ícone **Relatórios** na interface do Kaspersky Gadget (apenas no Microsoft Windows Vista e no Microsoft Windows 7).

   A guia **Relatório** exibe os relatórios de operação do aplicativo no formato de diagrama.

2. Se desejar exibir um relatório detalhado de operação do aplicativo (por exemplo, um relatório que represente a operação de cada componente), clique no botão **Relatório detalhado** na parte inferior da guia **Relatório**.

   A janela **Relatório detalhado** é aberta com os dados representados em uma tabela. Para obter uma exibição conveniente dos relatórios, é possível selecionar várias opções de classificação das entradas.

COMO RESTAURAR AS CONFIGURAÇÕES PADRÃO DO APLICATIVO

Você pode restaurar as configurações do Kaspersky Anti-Virus recomendadas pela Kaspersky Lab e consideradas ideais a qualquer momento. As configurações podem ser restauradas usando o *Assistente de Configuração do Aplicativo*.

Quando o Assistente concluir suas operações, o nível de segurança **Recomendado** estará definido para todos os componentes de proteção. Ao restaurar as configurações, também será solicitado que você defina as configurações que devem ou não ser mantidas para quais componentes ao restaurar o nível de segurança recomendado.

Para restaurar as configurações de proteção:

1. Abra a janela de configurações do aplicativo.
2. Execute o Assistente de Configuração do Aplicativo usando um dos métodos a seguir:
   - clique no link **Restaurar** na parte inferior da janela;
   - à esquerda da janela, selecione a seção **Configurações Avançadas**, subseção **Gerenciar Configurações** e clique no botão **Restaurar** na seção **Restaurar configurações padrão**.

As etapas detalhadas do Assistente.

Step 1. Iniciando o Assistente

Clique no botão **Avançar** para continuar com o Assistente.

Step 2. Selecionando as configurações que devem ser salvas

Esta janela do Assistente mostra os componentes do Kaspersky Anti-Virus cujas configurações são diferentes do valor padrão, por terem sido alteradas pelo usuário. Se tiverem sido criadas configurações especiais para algum componente, elas também serão mostradas na janela.

Marque as caixas correspondentes às configurações que você deseja salvar e clique no botão **Avançar**.

Step 3. Concluindo a restauração

Para concluir o Assistente, clique no botão **Concluir**.

COMO IMPORTAR AS CONFIGURAÇÕES DO APLICATIVO KASPERSKY ANTI-VIRUS INSTALADO EM OUTRO COMPUTADOR

Depois de configurar o produto, você poderá aplicar suas configurações ao Kaspersky Anti-Virus instalado em outro computador. Assim, o aplicativo será configurado da mesma maneira nos dois computadores. Esse recurso é útil quando, por exemplo, o Kaspersky Anti-Virus é instalado no seu computador doméstico e no seu escritório.

As configurações do aplicativo são armazenadas em um arquivo de configuração especial que pode ser transferido para outro computador. Para fazê-lo:

1. Execute o procedimento *Exportar* – salva as configurações do aplicativo em um arquivo de configuração.
2. Move o arquivo que você salvou em outro computador (por exemplo, envie-o por email ou use uma mídia de dados removível).
3. Execute o procedimento *Importar* – aplica as definições do arquivo de configuração ao aplicativo instalado em outro computador.

Para exportar as configurações atuais do Kaspersky Anti-Virus:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Gerenciar Configurações** à esquerda da janela.
3. Clique no botão **Salvar** à direita da janela.

4. Na janela que é aberta, insira o nome do arquivo de configuração e o caminho no qual ele deve ser salvo.

Para importar as configurações do aplicativo de um arquivo de configuração salvo:

1. Abra a janela de configurações do aplicativo.
2. Selecione a seção **Gerenciar Configurações** à esquerda da janela.
3. Clique no botão **Carregar** à direita da janela.
4. Na janela que é aberta, insira o arquivo do qual você deseja importar as configurações do Kaspersky Anti-Virus.

COMO ALTERNAR DO KASPERSKY ANTI-VIRUS PARA O KASPERSKY INTERNET SECURITY

O *Kaspersky Internet Security* é um aplicativo criado para assegurar a proteção abrangente do computador. É bastante semelhante ao Kaspersky Anti-Virus, mas apresenta diversas opções avançadas implementadas nos seguintes módulos de recursos:

- Controle de Aplicativos;
- Controle dos Pais;
- Firewall;
- Bloqueador de Ataques de Rede;
- Filtro Geográfico;
- Bloqueio do acesso a sites perigosos;
- Monitor de Rede;
- Antispam;
- Antibanner;
- Eliminação de rastros de atividade;
- Seção de Execução Segura.

Você pode alternar temporariamente para a versão de avaliação do Kaspersky Internet Security para se familiarizar com seus recursos ou passar imediatamente a usar a versão comercial do aplicativo.

Em determinadas regiões, ao usar uma licença com assinatura (consulte a seção "Status da assinatura" na página 148)ou trabalhar com o aplicativo, não é possível alterná-lo temporariamente para a versão de avaliação do Kaspersky Internet Security.

NESTA SEÇÃO:

Alternando para a versão comercial 72

Alternando temporariamente para a versão comercial 72

ALTERNANDO PARA A VERSÃO COMERCIAL

Se você deseja alternar para a versão comercial do Kaspersky Internet Security, não é necessário instalar o aplicativo. Você precisa apenas de um código de ativação da versão comercial do aplicativo que possa ser usado para ativar o aplicativo (consulte a seção "Como ativar o aplicativo" na página 55). Se já tiver uma licença comercial, você poderá obter o código de ativação.

Para comprar a licença comercial do Kaspersky Internet Security na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Atualizar** à esquerda da janela.
2. Clique no botão **Comprar Agora**.

   Ao concluir, você será redirecionado ao site da Loja Virtual, onde poderá comprar a licença comercial do Kaspersky Internet Security.

Em determinadas regiões, ao usar uma licença com assinatura (consulte a seção "Status da assinatura" na página 148) ou trabalhar com o aplicativo, a janela principal não contém a seção **Atualizar**.

ALTERNANDO TEMPORARIAMENTE PARA A VERSÃO COMERCIAL

Você pode alternar temporariamente para o Kaspersky Internet Security para avaliar seus recursos. Também é possível comprar uma licença para continuar usando o aplicativo.

Em determinadas regiões, ao usar uma licença com assinatura (consulte a seção "Status da assinatura" na página 148)ou trabalhar com o aplicativo, não é possível alterná-lo temporariamente para a versão de avaliação do Kaspersky Internet Security. Nesses casos, a janela principal do aplicativo não contém a seção **Atualizar**.

Para alternar temporariamente para o Kaspersky Internet Security na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Atualizar** à esquerda da janela.
2. Clique no botão **Experimentar Agora**.

   O Assistente de Configuração é iniciado no modo de atualização da proteção.

As etapas detalhadas do Assistente.

Step 1. Solicitar a ativação da versão de avaliação do Kaspersky Internet Security

Na primeira etapa, o Assistente envia uma solicitação ao servidor de ativação a fim de obter a permissão para ativar a versão de avaliação do Kaspersky Internet Security. Se a solicitação for enviada com êxito, o Assistente continuará automaticamente na etapa seguinte.

Step 2. Iniciando a implementação da proteção

Nesta etapa, o Assistente exibe uma mensagem notificando sobre a disponibilidade da atualização. Para continuar com o Assistente, clique no botão **Avançar**.

Step 3. Removendo aplicativos incompatíveis

Nesta etapa, o Assistente verifica se há aplicativos incompatíveis com o Kaspersky Internet Security instalados no computador. Se não for detectado nenhum aplicativo incompatível, o Assistente continuará automaticamente na etapa seguinte. Se forem detectados aplicativos incompatíveis, o Assistente os agrupará em uma lista que será exibida na janela com a opção de removê-los.

Depois que os aplicativos incompatíveis forem excluídos, talvez seja necessário reiniciar o sistema operacional. Depois de reiniciar o aplicativo, o Assistente será iniciado automaticamente e a atualização da proteção continuará.

Step 4. Atualizando a proteção

Nesta etapa, os módulos de atualização serão conectados, o que pode levar algum tempo. Quando o processo for concluído, o Assistente continuará automaticamente na próxima etapa.

Step 5. Reiniciando o aplicativo

Na etapa final da atualização do aplicativo, será necessário reiniciar o computador. Para fazer isso, clique no botão **Concluir** na janela do Assistente.

Step 6. Concluindo a ativação

Depois de reiniciar o aplicativo, o Assistente será iniciado automaticamente. Quando a versão de avaliação do Kaspersky Internet Security for ativada com êxito, a janela do Assistente exibirá informações sobre o período no qual você pode usar a versão de avaliação.

Step 7. Análise do sistema

Nesta etapa, são coletadas informações sobre os aplicativos do Microsoft Windows. Esses aplicativos são adicionados à lista de aplicativos confiáveis que não têm restrições sobre as ações que executam no sistema.

Quando a análise for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 8. Concluindo a atualização

Para concluir o Assistente, clique no botão **Concluir**.

Expiração do período de avaliação do Kaspersky Internet Security

Quando o período de avaliação do Kaspersky Internet Security expirar, o funcionamento de todos os componentes de proteção será interrompido. O aplicativo o notificará sobre esse evento.

Clique no botão **Reparar** na janela principal do aplicativo para selecionar um cenário de outras ações na janela do Assistente de Ativação que é aberta:

- Se você tiver uma licença comercial válida, volte a usar o Kaspersky Anti-Virus no modo padrão.
- Compre a licença comercial do Kaspersky Internet Security ou do Kaspersky Anti-Virus e ative o aplicativo (consulte a seção "Como ativar o aplicativo" na página 55).

Não é possível alternar temporariamente para o Kaspersky Internet Security uma segunda vez.

COMO USAR O KASPERSKY GADGET

Ao usar o Kaspersky Anti-Virus em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você também pode usar o Kaspersky Gadget (aqui chamado de *gadget*).

Depois de instalar o Kaspersky Anti-Virus em um computador com o Microsoft Windows 7, o gadget é exibido automaticamente na área de trabalho. Depois de instalar o aplicativo em um computador com o Microsoft Windows Vista, você deverá adicionar o gadget manualmente à Barra Lateral do Microsoft Windows (consulte a documentação do sistema operacional).

O indicador colorido do gadget exibe o status de proteção do computador da mesma forma que o indicador de status de proteção na janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44). O verde indica que o computador está totalmente protegido, o amarelo indica que há problemas com a proteção e o vermelho indica que a segurança do computador está em risco. A cor cinza indica que o aplicativo foi interrompido.

A aparência do gadget permite monitorar o download de atualizações: quando a atualização dos bancos de dados e módulos do aplicativo estão em andamento, é exibido um globo girando no centro do gadget.

Você pode usar o gadget para executar as seguintes tarefas principais:

- executar o aplicativo, caso ele tenha sido interrompido;
- abrir a janela principal do aplicativo;
- verificar objetos especificados quanto à presença de vírus;
- abrir a janela de notícias.

Para executar o aplicativo usando o gadget,

clique no ícone **Ativar** localizado no centro do gadget.

Para abrir a janela principal do aplicativo usando o gadget,

clique no ícone do Kaspersky Anti-Virus localizado no centro do gadget.

Para verificar um objeto quanto à presença de vírus usando o gadget,

arraste o objeto a ser verificado para o gadget.

O andamento da tarefa é exibido na janela **Verificação de Vírus** que é aberta.

Para abrir a janela de notícias usando o gadget,

clique no ícone exibido no centro do gadget quando for lançada alguma notícia.

Configurando o gadget

Você pode configurar o gadget para poder usar seus botões para iniciar as seguintes ações:

- editar as configurações do aplicativo;
- exibir os relatórios do aplicativo;
- pausar a proteção.

Além disso, você pode alterar a aparência do gadget selecionando outra capa para ele.

Para configurar o gadget:

1. Abra a janela de configurações do gadget clicando no ícone que será exibido no canto superior direito do bloco do gadget se você passar o ponteiro do mouse sobre ele.
2. Nas listas suspensas do **Ícone esquerdo** e do **Ícone direito**, selecione as ações que devem ser executadas ao clicar nos botões esquerdo e direito do gadget.
3. Selecione uma capa para o gadget clicando nos botões .
4. Clique no botão **OK** para salvar as alterações feitas.

CONFIGURAÇÕES AVANÇADAS DO APLICATIVO

Esta seção fornece informações detalhadas sobre cada componente do aplicativo e descreve os algoritmos de operação e configuração de cada componente.

Para ajustar as configurações avançadas do aplicativo, abra a janela de configurações usando um dos seguintes métodos:

- clique no botão **Configurações** na parte superior da janela principal do aplicativo;
- selecione **Configurações** no menu de contexto do ícone do aplicativo.

NESTA SEÇÃO:

Configurações de proteção geral 76

Verificação 77

Atualização 85

Antivírus de Arquivos 90

Antivírus de Email 96

Antivírus da Web 101

Antivírus de IM 108

Defesa Proativa 110

Inspetor do Sistema 112

Proteção de rede 114

Zona confiável 118

Desempenho e compatibilidade com outros aplicativos 119

Autodefesa do Kaspersky Anti-Virus 123

Quarentena e Backup 124

Ferramentas adicionais para proteger melhor seu computador 126

Relatórios 131

Exibição do aplicativo 135

Notificações 136

Participando do Kaspersky Security Network 138

CONFIGURAÇÕES DE PROTEÇÃO GERAL

Na janela de configurações do aplicativo, na subseção **Configurações Gerais** da seção **Centro de Proteção**, é possível executar as seguintes operações:

- desativar todos os componentes de proteção (consulte a seção "Ativando e desativando a proteção" na página 53);
- selecionar o modo de proteção interativa ou automática (consulte a seção "Selecionando o modo de proteção" na página 77);
- restringir o acesso dos usuários ao aplicativo definindo uma senha (consulte a seção "Restringindo o acesso ao Kaspersky Anti-Virus" na página 76);
- ativar ou desativar a execução automática do aplicativo ao iniciar o sistema operacional (consulte a seção "Ativando e desativando a execução automática" na página 50);
- ativar uma combinação de teclas personalizada para exibir o teclado virtual na tela (consulte a seção "Teclado Virtual" na página 62).

NESTA SEÇÃO:

Restringindo o acesso ao Kaspersky Anti-Virus 76

Selecionando o modo de proteção 77

RESTRINGINDO O ACESSO AO KASPERSKY ANTI-VIRUS

O computador pode ser usado por diversos usuários com níveis de experiência em computação diferentes. O acesso irrestrito ao Kaspersky Anti-Virus e suas configurações pode levar à redução no nível de proteção do computador.

Para restringir o acesso ao aplicativo, é possível definir uma senha e especificar as ações que exigem a inserção da senha:

- alteração das configurações do aplicativo;
- encerramento do aplicativo;
- remoção do aplicativo.

Use a senha para restringir o acesso à remoção do aplicativo com atenção. Se você esquecer a senha, será difícil remover o aplicativo do computador.

Para restringir o acesso ao Kaspersky Anti-Virus usando uma senha:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, selecione a seção **Centro de Proteção**, subseção **Configurações Gerais**.
3. À direita da janela, na seção **Proteção por senha**, marque a caixa **Ativar proteção por senha** e clique no botão **Configurações**.
4. Na janela **Proteção por senha** que é aberta, insira a senha e especifique a área que deve ser coberta pela restrição de acesso.

SELECIONANDO O MODO DE PROTEÇÃO

Por padrão, o Kaspersky Anti-Virus é executado no *modo de proteção automática*. Nesse modo, o aplicativo aplica automaticamente as ações recomendadas pela Kaspersky Lab em resposta a eventos perigosos. Se desejar ser notificado pelo Kaspersky Anti-Virus sobre todos os eventos perigosos e suspeitos no sistema e poder decidir quais das ações oferecidas pelo aplicativo devem ser aplicadas, você pode ativar o *modo de proteção interativa*.

Para selecionar o modo de proteção:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione a subseção **Configurações Gerais**.
3. Na seção **Proteção interativa**, marque ou desmarque as caixas de acordo com o modo de proteção selecionado:
   - para ativar o modo de proteção interativa, desmarque **Selecionar ação automaticamente**;
   - para ativar o modo de proteção automática, marque **Selecionar ação automaticamente**.

     Se não desejar que o Kaspersky Anti-Virus exclua os objetos suspeitos ao ser executado no modo automático, marque a caixa **Não excluir objetos suspeitos**.

VERIFICAÇÃO

A verificação do computador quanto à presença de vírus e vulnerabilidades é uma das tarefas mais importantes para garantir a segurança do computador. Isso é necessário para verificar periodicamente o computador quanto à presença de vírus e descartar a possibilidade de disseminação de programas maliciosos que não foram descobertos pelos componentes de segurança porque, por exemplo, o nível de segurança está com uma definição baixa ou por outros motivos.

A verificação de vulnerabilidades executa o diagnóstico do sistema operacional e detecta recursos de software que podem ser usados por invasores para disseminar objetos maliciosos e obter acesso a informações pessoais.

As seções a seguir contêm informações detalhadas sobre os recursos e a configuração das tarefas de verificação, níveis de segurança, métodos e tecnologias de verificação.

NESTA SEÇÃO:

Verificação de vírus 77

Verificação de Vulnerabilidades 85

VERIFICAÇÃO DE VÍRUS

O Kaspersky Anti-Virus compreende as seguintes tarefas de verificação de objetos quanto à presença de vírus:

- **Verificação Personalizada**. Verificação de objetos selecionados pelo usuário. Você pode verificar os seguintes objetos do sistema de arquivos do computador: memória do sistema, objetos carregados na inicialização, backup do sistema, bancos de dados de email, discos rígidos, mídias de armazenamento removível e unidades de rede.
- **Verificação completa**. Uma verificação completa de todo o sistema. Por padrão, os seguintes objetos são verificados: memória do sistema, objetos carregados na inicialização, backup do sistema, bancos de dados de email, discos rígidos, mídias de armazenamento removível e unidades de rede.

- **Verificação de Áreas Críticas**. Verificação de vírus nos objetos de inicialização do sistema operacional.

As tarefas Verificação Completa e Verificação de Áreas Críticas têm características específicas. Para essas verificações, não é recomendável editar as listas de objetos que devem ser verificados.

Cada tarefa de verificação é executada na área especificada e pode ser executada de acordo com a programação criada. Cada tarefa de verificação se caracteriza por seu nível de segurança (combinação de configurações que afetam a profundidade da verificação). Por padrão, o modo de uso de registros dos bancos de dados do aplicativo para procurar ameaças está sempre ativado. Além disso, você pode aplicar diversos métodos e tecnologias de verificação (veja a página 81).

Depois de executar a tarefa de verificação completa ou de verificação de áreas críticas, o andamento de execução da tarefa será exibido na seção **Verificação** da janela principal do Kaspersky Anti-Virus, no campo sob o nome da tarefa em execução.

Se for detectada uma ameaça, o Kaspersky Anti-Virus atribuirá um dos seguintes status ao objeto encontrado:

- programa malicioso (como um *vírus* ou um *cavalo de Troia*);
- *possivelmente infectado* (suspeito), quando a verificação não puder determinar se o objeto está infectado ou não. O arquivo pode conter uma sequência de código adequada aos vírus ou o código modificado de um vírus conhecido.

O aplicativo exibe uma notificação sobre a ameaça detectada e executa a ação atribuída. Você pode alterar as ações que devem ser executadas com as ameaças detectadas.

Se estiver trabalhando no modo automático (consulte a seção "Selecionando o modo de proteção" na página 77), o Kaspersky Anti-Virus aplicará automaticamente a ação recomendada pelos especialistas da Kaspersky Lab ao detectar objetos perigosos. Para objetos maliciosos, a ação é **Desinfetar. Excluir se a desinfecção falhar** e, para objetos suspeitos, é **Mover para a Quarentena**.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup para posterior restauração ou desinfecção. Os objetos suspeitos (possivelmente infectados) são colocados em quarentena. Você pode ativar a verificação de objetos em quarentena após cada atualização.

As informações sobre os resultados e eventos da verificação ocorridos durante a execução da tarefa são registrados em um relatório do Kaspersky Anti-Virus.

CONSULTE TAMBÉM:

Como executar a verificação completa do computador quanto à presença de vírus

Como verificar as áreas críticas do computador quanto à presença de vírus

Como verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus

NESTA SEÇÃO:

Alterando e restaurando o nível de segurança

Criando a programação de inicialização da verificação

Criando uma lista de objetos a serem verificados

Selecionando o método de verificação

Selecionando a tecnologia de verificação

Alterando as ações a serem executadas com os objetos detectados

Executando a verificação com outra conta de usuário

Alterando o tipo de objetos a serem verificados

Verificação de arquivos compostos

Otimização da verificação

Verificando unidades removíveis ao conectar

Criando um atalho de tarefa

ALTERANDO E RESTAURANDO O NÍVEL DE SEGURANÇA

Dependendo de suas necessidades atuais, é possível selecionar um dos níveis de segurança predefinidos ou modificar manualmente as configurações da verificação.

Ao configurar a tarefa de verificação, você pode reverter para a configuração recomendada a qualquer momento. Elas são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

- *Para alterar o nível de segurança definido, execute as seguintes ações:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, defina o nível de segurança necessário para a tarefa selecionada ou clique no botão **Configurações** para modificar as configurações manualmente.

Se você modificar as configurações manualmente, o nome do nível de segurança será alterado para **Personalizado**.

- *Para restaurar as configurações de verificação padrão:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Nível padrão** da tarefa selecionada.

CRIANDO A PROGRAMAÇÃO DE INICIALIZAÇÃO DA VERIFICAÇÃO

Você pode criar uma programação para iniciar automaticamente as tarefas de verificação de vírus: especificar a frequência de execução da tarefa, a hora de início (se necessário) e configurações avançadas.

Se por algum motivo não for possível executar a tarefa (por exemplo, se o computador não estiver ligado naquela hora), você poderá configurar a tarefa ignorada para ser iniciada automaticamente assim que possível. Você pode pausar a verificação automaticamente quando a proteção de tela está inativa ou o computador está desbloqueado. Essa funcionalidade adia a execução até que o usuário tenha concluído seu trabalho no computador. Então, verificação não utilizará recursos do sistema durante o trabalho.

O modo de Verificação Ociosa especial (consulte a seção "Executando tarefas em background" na página 121) permite iniciar a verificação da memória do sistema, da partição do sistema e dos objetos de inicialização mantendo seu computador ocioso.

Para modificar a programação das tarefas de verificação:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por Programação** e configure o modo de execução da verificação.

Para ativar a execução automática da tarefa ignorada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por programação** e marque a caixa **Executar tarefas ignoradas**.

Para executar as tarefas somente quando o computador não estiver em uso:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por programação** e marque a caixa **Pausar a verificação programada quando a proteção de tela estiver inativa e o computador estiver desbloqueado**.

CRIANDO UMA LISTA DE OBJETOS A SEREM VERIFICADOS

Cada tarefa de verificação de vírus possui sua própria lista de objetos padrão. Esses objetos podem incluir itens do sistema de arquivos do computador, como unidades lógicas e **bancos de dados de email**, ou outros tipos de objetos, como unidades de rede. É possível editar essa lista.

Se o escopo da verificação estiver vazio ou não contiver nenhum objeto selecionado, a tarefa de verificação não poderá

ser iniciada.

- *Para criar uma lista de objetos para uma tarefa de verificação de objetos:*

  1. Abra a janela principal do aplicativo.
  2. À esquerda da janela, selecione a seção **Verificação**.
  3. À direita da janela, clique no link **selecionar** para abrir a lista de objetos para a verificação.
  4. Na janela **Verificação Personalizada** que é aberta, clique no botão **Adicionar**.
  5. Na janela **Selecionar objeto a ser verificado** que é aberta, selecione o objeto desejado e clique no botão **Adicionar**. Clique no botão **OK** depois de adicionar todos os objetos desejados. Para excluir objetos da lista de objetos a serem verificados, desmarque as caixas ao lado deles.

     Você também pode arrastar os arquivos que devem ser verificados diretamente na área marcada localizada na seção **Verificação**.

- *Para criar a lista de objetos para as tarefas Verificação Completa, Verificação de Áreas Críticas ou Verificação de Vulnerabilidades:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
  3. À direita da janela, clique no botão **Escopo da verificação**.
  4. Na janela **Escopo da verificação** que é aberta, use os botões **Adicionar**, **Editar** e **Excluir** para criar uma lista. Para excluir objetos da lista de objetos a serem verificados, desmarque as caixas ao lado deles.

     Por padrão, não é possível editar ou excluir os objetos que aparecem na lista.

SELECIONANDO O MÉTODO DE VERIFICAÇÃO

Durante a verificação de vírus, a *análise de assinaturas* é usada sempre: O Kaspersky Anti-Virus compara o objeto encontrado com os registros do banco de dados.

Você pode usar os métodos de verificação adicionais para aumentar a eficiência da verificação: a *análise heurística* (análise das ações executadas por um objeto no sistema) e a *verificação de rootkits* (ferramentas que podem ocultar programas maliciosos no sistema operacional).

- *Para especificar o método de verificação a ser usado:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
  3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
  4. Na janela que é aberta, na guia **Adicional**, na seção **Métodos de verificação**, selecione os valores desejados das configurações.

SELECIONANDO A TECNOLOGIA DE VERIFICAÇÃO

Além dos métodos de verificação, você pode usar tecnologias especiais que permitem aumentar a velocidade da verificação de vírus através da exclusão dos arquivos que não foram modificados desde sua última verificação.

Para ativar as tecnologias de verificação de objetos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
4. Na janela que é aberta, na guia **Adicional**, na seção **Tecnologias de verificação**, selecione os valores desejados.

ALTERANDO AS AÇÕES A SEREM EXECUTADAS COM OS OBJETOS DETECTADOS

Quando são detectados objetos infectados ou possivelmente infectados, o aplicativo executa a ação especificada.

Para alterar a ação a ser executada com os objetos detectados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. À direita da janela, na seção **Ação ao detectar ameaça**, selecione a opção desejada.

EXECUTANDO A VERIFICAÇÃO COM OUTRA CONTA DE USUÁRIO

Por padrão, as tarefas de verificação são executadas com sua conta do sistema. Porém, talvez seja necessário executar a tarefa com outra conta de usuário. Você pode especificar a conta que deve ser usada pelo aplicativo ao executar uma tarefa de verificação.

Para iniciar a verificação com outra conta de usuário:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas**, **Verificação Personalizada** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Conta do usuário**, marque a caixa **Executar tarefa como**. Especifique o nome do usuário e a senha.

ALTERANDO O TIPO DE OBJETOS A SEREM VERIFICADOS

Ao especificar os tipos de objetos a serem verificados, você estabelece os formatos e tamanhos de arquivos que serão verificados quanto à presença de vírus ao executar a tarefa de verificação selecionada.

Ao selecionar os tipos de arquivos, lembre-se do seguinte:

- A probabilidade de infiltração de código malicioso em diversos formatos de arquivo (como .txt) e sua ativação posterior é bastante pequena. Ao mesmo tempo, há formatos que contêm ou que podem conter um código executável (como exe, dll, doc). O risco de infiltração e ativação de código malicioso nesses arquivos é bastante alto.
- O invasor pode enviar ao seu computador um vírus em um arquivo executável renomeado como um arquivo txt. Se você selecionou a opção verificação de arquivos por extensão, esse arquivo será ignorado pela verificação. Se a verificação de arquivos por formato foi selecionada, então, independentemente da extensão, o Antivírus

de Arquivos analisará o cabeçalho do arquivo e descobrirá que trata-se de um arquivo .exe. Esse arquivo seria verificado cuidadosamente quanto à presença de vírus.

Para alterar os tipos de objetos verificados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
4. Na janela que é aberta, na guia **Escopo**, na seção **Tipos de arquivos**, selecione a opção desejada.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS

Um método comum para ocultar vírus é incorporá-los em arquivos compostos, como arquivos comprimidos, bancos de dados, etc. Para detectar vírus que estão ocultos dessa forma, é necessário descompactar os arquivos compostos, o que pode reduzir significativamente a velocidade da verificação.

Para cada tipo de arquivo composto, você pode selecionar a verificação de todos os arquivos ou apenas dos arquivos novos. Para selecionar, clique no link ao lado do nome do objeto. Seu valor é mudado quando você clica nele. Se você selecionar o modo de verificação apenas de arquivos novos e modificados (veja a página 84), não poderá selecionar os links que permitem verificar todos os arquivos ou apenas os arquivos novos.

Você pode limitar o tamanho máximo do arquivo composto verificado. Os arquivos compostos maiores que o tamanho especificado não serão verificados.

Quando arquivos grandes são extraídos de arquivos comprimidos, eles são verificados mesmo que a caixa **Não descompactar arquivos compostos grandes** esteja marcada.

Para modificar a lista de arquivos compostos verificados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
4. Na janela que é aberta, na guia **Escopo**, na seção **Verificação de arquivos compostos**, selecione os tipos de arquivos compostos que devem ser verificados.

Para definir o tamanho máximo dos arquivos compostos a serem verificados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
4. Na janela que é aberta, na guia **Escopo**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.
5. Na janela **Arquivos compostos** que é aberta, marque a caixa **Não descompactar arquivos compostos grandes** e especifique o tamanho máximo de arquivo.

OTIMIZAÇÃO DA VERIFICAÇÃO

Você pode reduzir o tempo de verificação e aumentar a velocidade do Kaspersky Anti-Virus. Isso é possível verificando apenas os arquivos novos e aqueles que foram alterados desde a última vez que foram verificados. Esse modo se aplica a arquivos simples e compostos.

Você também pode definir uma restrição sobre a duração da verificação de um objeto. Quando o intervalo de tempo especificado acabar, o objeto será excluído da verificação atual (exceto os arquivos comprimidos e os arquivos compostos por vários objetos).

- *Para verificar somente arquivos novos e alterados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
  3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
  4. Na janela que é aberta, na guia **Escopo**, na seção **Otimização da verificação**, marque a caixa **Verificar somente arquivos novos e alterados**.

- *Para definir uma restrição sobre a duração da verificação:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
  3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
  4. Na janela que é aberta, na guia **Escopo**, na seção **Otimização da verificação**, marque a caixa **Ignorar objetos verificados por mais de** e especifique a duração da verificação de um único arquivo.

VERIFICANDO UNIDADES REMOVÍVEIS AO CONECTAR

Atualmente, os objetos maliciosos que usam vulnerabilidades dos sistemas operacionais para se replicar através das redes e mídias removíveis estão cada vez mais difundidos. O Kaspersky Anti-Virus permite verificar as unidades removíveis ao conectá-las ao computador.

- *Para configurar a verificação de mídias removíveis ao conectar:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione **Configurações Gerais**.
  3. Na seção **Verificar unidades removíveis ao conectar**, selecione a ação e defina o tamanho máximo da unidade a ser conectada no campo abaixo, se necessário.

CRIANDO UM ATALHO DE TAREFA

O aplicativo oferece a opção de criar atalhos para o início rápido de tarefas de verificação completa, rápida e de vulnerabilidades. Isso permite iniciar a verificação desejada sem abrir a janela principal do aplicativo ou o menu de contexto.

- *Para criar um atalho para iniciar uma verificação:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione **Configurações Gerais**.

3. À direita da janela, na seção **Execução rápida de tarefas de verificação**, clique no botão **Criar atalho** ao lado do nome da tarefa desejada (**Verificação de Áreas Críticas**, **Verificação Completa** ou **Verificação de Vulnerabilidades**).

4. Especifique o caminho para salvar o atalho e seu nome na janela que é aberta. Por padrão, o atalho será criado com o nome da tarefa na pasta *Meu computador* do usuário do computador atual.

VERIFICAÇÃO DE VULNERABILIDADES

As vulnerabilidades do sistema operacional podem ser causadas por erros de programação ou de engenharia, senhas não confiáveis, atividade de programas maliciosos e outros. Ao verificar vulnerabilidades, o aplicativo analisa o sistema, pesquisa anomalias e configurações danificadas do sistema operacional e do navegador da Web, procura serviços vulneráveis e adota outras precauções relacionadas à segurança.

O diagnóstico pode levar algum tempo. Quando ele for concluído, os problemas encontrados serão analisados considerando uma possível ameaça ao sistema.

Depois de iniciar a tarefa de verificação de vulnerabilidades (veja a página 61), seu andamento será exibido na janela **Verificação de Vulnerabilidades**, no campo **Concluir**. As vulnerabilidades detectadas ao verificar o sistema e os aplicativos são exibidas na mesma janela, nas guias **Vulnerabilidades do sistema** e **Aplicativos vulneráveis**.

Ao pesquisar ameaças, as informações sobre os resultados são registradas em um relatório do Kaspersky Anti-Virus.

Da mesma forma que com as tarefas de verificação de vírus, você pode definir uma programação de inicialização da tarefa de verificação de vulnerabilidades, criar uma lista de objetos a serem verificados (veja a página 80), especificar uma conta (consulte a seção "Executando a verificação com outra conta de usuário" na página 82) e criar um atalho para a execução rápida de uma tarefa. Por padrão, os aplicativos já instalados no computador são selecionados como objetos de verificação.

ATUALIZAÇÃO

A atualização dos bancos de dados e módulos do programa do Kaspersky Anti-Virus garantem o status de proteção atualizado do computador. Diariamente aparecem novos vírus, cavalos de Troia e outros tipos de malware em todo o mundo. Os bancos de dados do Kaspersky Anti-Virus contêm informações sobre ameaças e maneiras para eliminá-las, de forma que a atualização periódica do aplicativo é necessária para garantir a segurança do computador e a detecção oportuna de novas ameaças.

A atualização periódica exige uma licença ativa para usar o aplicativo. Sem uma licença, você poderá atualizar o aplicativo apenas uma vez.

A atualização do aplicativo baixa e instala as seguintes atualizações no seu computador:

- Bancos de dados do Kaspersky Anti-Virus.

  A proteção das informações se baseia nos bancos de dados que contêm assinaturas de ameaças e de ataques de rede, além dos métodos usados para combatê-los. Os componentes de proteção usam esses bancos de dados para pesquisar e desinfetar objetos perigosos no computador. Os bancos de dados são complementados a cada hora com registros de novas ameaças. Assim, é recomendável atualizá-los periodicamente.

  Além dos bancos de dados do Kaspersky Anti-Virus, os drivers de rede que ativam os componentes do aplicativo para interceptar o tráfego de rede são atualizados.

- Módulos do aplicativo.

  Além dos bancos de dados do Kaspersky Anti-Virus, você também pode atualizar os módulos do programa. Os pacotes de atualização corrigem as vulnerabilidades do Kaspersky Anti-Virus e acrescentam ou melhoram as funcionalidades existentes.

A principal fonte de atualização do Kaspersky Anti-Virus são os servidores de atualização especiais da Kaspersky Lab. Ao atualizar o Kaspersky Anti-Virus, você pode copiar as atualizações dos bancos de dados e módulos do programa recebidos dos servidores da Kaspersky Lab em uma pasta local que dá acesso a outros computadores da rede. Isso economiza tráfego da Internet.

Você também pode modificar as configurações de execução automática da atualização.

O computador deve estar conectado com a Internet para baixar com êxito as atualizações dos nossos servidores. Por padrão, as configurações da conexão com a Internet são determinadas automaticamente. Se você usar um servidor proxy, talvez seja necessário ajustar as configurações de conexão.

Durante uma atualização (veja a página 116), os bancos de dados e módulos do aplicativo do computador são comparados com a versão atualizada na fonte de atualização. Se os bancos de dados e módulos atuais forem diferentes daqueles na versão real do aplicativo, a parte das atualizações que falta será instalada no computador.

Se os bancos de dados estiverem desatualizados, o pacote de atualização pode ser grande, o que gerará um tráfego de Internet adicional (de até várias dezenas de Mb).

Antes de atualizar os bancos de dados, o Kaspersky Anti-Virus cria cópias de backup dos mesmos, caso depois você queira reverter para a versão anterior dos bancos de dados.

As informações sobre as condições atuais dos bancos de dados do Kaspersky Anti-Virus são exibidas na seção **Atualização** da janela principal do aplicativo.

As informações sobre os resultados e eventos da atualização ocorridos durante a execução da tarefa de atualização são registrados em um relatório do Kaspersky Anti-Virus.

NESTA SEÇÃO:

Selecionando uma fonte de atualização 86

Criando a programação de inicialização da atualização 88

Revertendo a última atualização 89

Verificando a Quarentena após a atualização..... 89

Usando o servidor proxy 89

Executando atualizações com outra conta de usuário 90

SELECIONANDO UMA FONTE DE ATUALIZAÇÃO

A *fonte de atualização* é um recurso que contém as atualizações dos bancos de dados e dos módulos do Kaspersky Anti-Virus. Você pode especificar servidores HTTP/FTP, pastas locais e de rede como fontes de atualização.

As principais fontes de atualização são os servidores de atualização da Kaspersky Lab, nos quais são armazenadas atualizações do banco de dados e do módulo do aplicativo de todos os produtos da Kaspersky Lab.

Se você não tem acesso aos servidores de atualização da Kaspersky Lab (por exemplo, seu acesso à Internet é limitado), é possível ligar para a sede da Kaspersky Lab (http://brazil.kaspersky.com/suporte/informa%C3%A7%C3%B5es-de-contato-do-suporte-para-usu%C3%A1rios-dom%C3%A9sticos) para solicitar informações de contato dos parceiros da Kaspersky Lab, que podem fornecer atualizações em mídia removível.

Ao solicitar atualizações em mídia removível, especifique se deseja receber também as atualizações dos módulos do aplicativo.

Por padrão, a lista de fontes de atualização contém apenas os servidores de atualização da Kaspersky Lab. Se vários recursos forem selecionados como fontes de atualização, o Kaspersky Anti-Virus tentará se conectar a cada um deles, começando pelo primeiro na lista, e recuperará as atualizações da primeira fonte disponível.

Se um recurso externo à rede local for selecionado como fonte de atualização, é necessário ter uma conexão com a internet para a atualização.

Para escolher uma fonte de atualização:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Fonte de atualização** à direita da janela.
4. Na janela que é aberta, na guia **Fonte**, abra a janela de seleção clicando no botão **Adicionar**.
5. Na janela **Selecionar fonte de atualização** que é aberta, selecione uma pasta que contém as atualizações ou insira um endereço no campo **Fonte** para especificar o servidor do qual as atualizações devem ser baixadas.

SELECIONANDO A REGIÃO DO SERVIDOR DE ATUALIZAÇÃO

Se você usar os servidores da Kaspersky Lab como fonte de atualização, poderá selecionar o local do servidor ideal para o download das atualizações. Os servidores da Kaspersky Lab estão localizados em diversos países.

O uso do servidor de atualização da Kaspersky Lab mais próximo permite reduzir o tempo necessário para receber as atualizações e aumentar a velocidade de desempenho da operação. Por padrão, o aplicativo usa as informações sobre a região atual contidas no Registro do sistema operacional. Você pode selecionar a região manualmente.

Para selecionar a região do servidor:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Fonte de atualização** à direita da janela.
4. Na janela que é aberta, na guia **Fonte**, na seção **Configurações regionais**, selecione a opção **Selecionar na lista** e, em seguida, selecione o país mais próximo do seu local atual na lista suspensa.

ATUALIZANDO O APLICATIVO DE UMA PASTA COMPARTILHADA

Para economizar tráfego da Internet, é possível configurar a atualização do Kaspersky Anti-Virus a partir de uma pasta compartilhada ao atualizar o aplicativo em computadores em rede. Nesse caso, um dos computadores em rede recebe um pacote de atualização dos servidores da Kaspersky Lab ou de outro recurso da Web que contenha o conjunto de atualizações necessário. As atualizações recebidas são copiadas em uma pasta compartilhada. Os outros computadores da rede acessam essa pasta para receber as atualizações do Kaspersky Anti-Virus.

Para ativar o modo de distribuição de atualizações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Marque a caixa **Copiar atualizações para pasta** na seção **Adicional** e, no campo abaixo, especifique o caminho da pasta pública na qual todas as atualizações baixadas serão copiadas. Você também pode selecionar uma pasta clicando no botão **Procurar**.

Para ativer a atualização do aplicativo em um determinado computador a partir da pasta compartilhada selecionada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Fonte de atualização** à direita da janela.
4. Na janela que é aberta, na guia **Fonte**, abra a janela de seleção clicando no botão **Adicionar**.
5. Na janela **Selecionar fonte de atualização** que é aberta, selecione uma pasta ou insira seu caminho completo no campo **Fonte**.
6. Desmarque a caixa **Servidores de atualização da Kaspersky Lab** na guia **Fonte**.

CRIANDO A PROGRAMAÇÃO DE INICIALIZAÇÃO DA VERIFICAÇÃO

Você pode criar uma programação para iniciar uma tarefa de atualização automaticamente: especificar a frequência de execução da tarefa, a hora de início (se necessário) e configurações avançadas.

Se por algum motivo não for possível executar a tarefa (por exemplo, se o computador não estiver ligado naquela hora), você poderá configurar a tarefa ignorada para ser iniciada automaticamente assim que possível.

Você também pode adiar o início automático da tarefa depois que o aplicativo é iniciado. Todas as tarefas programadas serão executadas somente depois de decorrido o intervalo de tempo especificado desde o início do Kaspersky Anti-Virus.

O modo de Verificação Ociosa especial (consulte a seção "Executando tarefas em background" na página 121) permite iniciar as atualizações automáticas mantendo o computador ocioso.

Para configurar a programação de inicialização da tarefa de atualização:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione a opção **Por programação** e configure o modo de execução da atualização.

Para ativar a execução automática da tarefa ignorada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por programação** e marque a caixa **Executar tarefas ignoradas**.

Para adiar a execução da tarefa após o início do aplicativo:

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.

3. Clique no botão **Modo de execução** à direita da janela.

4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione a opção **Por programação** e preencha o campo **Adiar a execução após o início do aplicativo por** para especificar o tempo pelo qual a execução da tarefa deve ser adiada.

REVERTENDO A ÚLTIMA ATUALIZAÇÃO

Depois da primeira atualização dos bancos de dados e módulos do programa do Kaspersky Anti-Virus, fica disponível a opção de reverter para os bancos de dados anteriores.

No início do processo de atualização, o Kaspersky Anti-Virus cria uma cópia de backup dos bancos de dados e módulos do programa atuais. Se necessário, é possível restaurar os bancos de dados anteriores. O recurso de reversão das atualizações pode ser útil caso a nova versão dos bancos de dados contenha uma assinatura inválida, o que faria o Kaspersky Anti-Virus bloquear um aplicativo seguro.

Se o banco de dados do Kaspersky Anti-Virus estiver corrompido, é recomendável executar a tarefa de atualização para baixar um conjunto válido de bancos de dados e ter uma proteção atualizada.

Para reverter para a versão anterior do banco de dados:

1. Abra a janela principal do aplicativo.

2. Selecione a seção **Centro de Atualizações** à esquerda da janela.

3. Clique no botão **Reverter para os bancos de dados anteriores** à direita da janela.

VERIFICANDO A QUARENTENA APÓS A ATUALIZAÇÃO

Se o aplicativo tiver verificado um objeto e não descobriu quais programas maliciosos o infectaram, o objeto será colocado na Quarentena. É possível que, após a próxima atualização dos bancos de dados, o produto possa reconhecer a ameaça com segurança e neutralizá-la. Você pode ativar a verificação automática de objetos em quarentena após cada atualização.

Por isso, o aplicativo verifica os objetos da Quarentena após cada atualização. A verificação pode alterar seus status. Alguns objetos poderão ser então restaurados para os locais anteriores e você poderá continuar trabalhando com eles.

Para ativar a verificação dos arquivos da Quarentena após a atualização:

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.

3. Marque a caixa **Verificar a Quarentena novamente após a atualização** na seção **Adicional**.

USANDO O SERVIDOR PROXY

Se você usar um servidor proxy para a conexão com a Internet, reconfigure-o para permitir a atualização adequada do Kaspersky Anti-Virus.

Para configurar o servidor proxy:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Fonte de atualização** à direita da janela.
4. Na janela que é aberta, na guia **Fonte**, clique no botão **Servidor proxy**.
5. Configure o servidor proxy na janela **Configurações do servidor proxy** que é aberta.

EXECUTANDO ATUALIZAÇÕES COM OUTRA CONTA DE USUÁRIO

Por padrão, o procedimento de atualização é executado com sua conta do sistema. No entanto, o Kaspersky Anti-Virus pode ser atualizado a partir de uma fonte na qual você não tem direitos de acesso (por exemplo, de uma pasta de rede que contém as atualizações) ou credenciais de usuário proxy que exige autorização. Você pode executar as atualizações do Kaspersky Anti-Virus em nome de uma conta de usuário que possua esses direitos.

Para iniciar a atualização com uma conta de usuário diferente:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Atualizações**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Conta do usuário**, marque a caixa **Executar tarefa como**. Especifique o nome do usuário e a senha.

ANTIVÍRUS DE ARQUIVOS

O Antivírus de Arquivos evita a infecção do sistema de arquivos do computador. O componente é executado ao iniciar o sistema operacional, permanece continuamente na RAM do computador e verifica todos os arquivos abertos, gravados ou executados no computador e em todas as unidades conectadas.

Você pode criar o escopo de proteção e definir o nível de segurança (coleção de configurações que determinam a profundidade da verificação).

Quando o usuário ou um programa tenta acessar um arquivo protegido, o Antivírus de Arquivos verifica se os bancos de dados do iChecker e do iSwift contêm informações sobre o arquivo e decide se ele deve ser verificado ou não.

Por padrão, o modo de uso de registros dos bancos de dados do aplicativo para procurar ameaças está sempre ativado. Além disso, é possível aplicar a análise heurística (veja a página 94) e diversas tecnologias de verificação (veja a página 94).

Se for detectada uma ameaça, o Kaspersky Anti-Virus atribuirá um dos seguintes status ao objeto encontrado:

- programa malicioso (como um *vírus* ou um *cavalo de Troia*);
- *possivelmente infectado* (suspeito), quando a verificação não puder determinar se o objeto está infectado ou não. O arquivo pode conter uma sequência de código adequada aos vírus ou o código modificado de um vírus conhecido.

O aplicativo exibe uma notificação sobre a ameaça detectada e executa a ação atribuída. Você pode alterar as ações que devem ser executadas com as ameaças detectadas.

Se estiver trabalhando no modo automático (consulte a seção "Selecionando o modo de proteção" na página 77), o Kaspersky Anti-Virus aplicará automaticamente a ação recomendada pelos especialistas da Kaspersky Lab ao detectar objetos perigosos. Para objetos maliciosos, a ação é **Desinfetar. Excluir se a desinfecção falhar** e, para objetos suspeitos, é **Mover para a Quarentena**.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup para posterior restauração ou desinfecção. Os objetos suspeitos (possivelmente infectados) são colocados em quarentena. Você pode ativar a verificação de objetos em quarentena após cada atualização.

NESTA SEÇÃO:

Ativando e desativando o Antivírus de Arquivos 91

Pausando o Antivírus de Arquivos automaticamente 91

Criando um escopo de proteção 92

Alterando e restaurando o nível de segurança 93

Selecionando o modo de verificação 93

Usando a análise heurística 94

Selecionando a tecnologia de verificação 94

Alterando as ações a serem executadas com os objetos detectados 94

Verificação de arquivos compostos 95

Otimização da verificação 96

ATIVANDO E DESATIVANDO O ANTIVÍRUS DE ARQUIVOS

Por padrão, o Antivírus de Arquivos está ativado, funcionando no modo normal. Se necessário, você pode desativar o Antivírus de Arquivos.

Para desativar o Antivírus de Arquivos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. À direita da janela, desmarque a caixa **Ativar Antivírus de Arquivos**.

PAUSANDO O ANTIVÍRUS DE ARQUIVOS AUTOMATICAMENTE

Ao realizar trabalhos que utilizam muitos recursos, você pode pausar o Antivírus de Arquivos. Para reduzir a carga de trabalho e assegurar o rápido acesso aos objetos, você pode configurar a pausa automática do componente em uma hora especificada ou ao trabalhar com determinados programas.

Pausar o Antivírus de Arquivos quando ele estiver em conflito com outro programa é uma operação emergencial! Se houver conflitos ao trabalhar com o componente, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab (http://brazil.kaspersky.com/suporte/). Os especialistas em suporte ajudarão a solucionar a operação simultânea do Kaspersky Anti-Virus com outros aplicativos no computador.

Para pausar o componente em uma hora especificada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.
4. Na janela que é aberta, na guia **Adicional**, na seção **Pausar tarefa**, marque a caixa **Por programação** e clique no botão **Programar**.
5. Na janela **Pausar tarefa**, especifique a hora (no formato de 24 horas hh:mm) em que a proteção será pausada (campos **Pausar tarefa às** e **Reiniciar tarefa às**).

Para pausar o componente ao executar determinados aplicativos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.
4. Na janela que é aberta, na guia **Adicional**, na seção **Pausar tarefa**, marque a caixa **Ao iniciar o aplicativo** e clique no botão **Selecionar**.
5. Na janela **Aplicativos**, crie uma lista de aplicativos cuja execução pausará o componente.

CRIANDO UM ESCOPO DE PROTEÇÃO

O escopo de proteção consiste no local dos objetos e no tipo de arquivos que devem ser verificados. Por padrão, o Kaspersky Anti-Virus verifica apenas os arquivos que podem ser infectados armazenados em qualquer disco rígido, unidade de rede ou mídia removível.

Você pode ampliar ou restringir o escopo de proteção adicionando/removendo objetos a serem verificados, ou alterando os tipos de arquivos a serem verificados. Por exemplo, você pode selecionar apenas os arquivos EXE executados de unidades de rede para serem verificados.

Ao selecionar os tipos de arquivos, lembre-se do seguinte:

- A probabilidade de infiltração de código malicioso em diversos formatos de arquivo (como .txt) e sua ativação posterior é bastante pequena. Ao mesmo tempo, há formatos que contêm ou que podem conter um código executável (como exe, dll, doc). O risco de infiltração e ativação de código malicioso nesses arquivos é bastante alto.
- O invasor pode enviar ao seu computador um vírus em um arquivo executável renomeado como um arquivo txt. Se você selecionou a opção verificação de arquivos por extensão, esse arquivo será ignorado pela verificação. Se a verificação de arquivos por formato foi selecionada, então, independentemente da extensão, o Antivírus de Arquivos analisará o cabeçalho do arquivo e descobrirá que trata-se de um arquivo .exe. Esse arquivo seria verificado cuidadosamente quanto à presença de vírus.

Para editar a lista de verificação de objetos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela que é aberta, na guia **Geral**, na seção **Escopo de proteção**, abra a janela de seleção de objetos clicando no link **Adicionar**.
5. Na janela **Selecionar objeto a ser verificado**, selecione o objeto e clique no botão **Adicionar**.

6. Depois de adicionar todos os objetos desejados, clique no botão **OK** na janela **Selecionar objeto a ser verificado**.

7. Para remover um objeto da lista de verificação, desmarque a caixa ao lado de seu nome.

- *Para alterar os tipos de objetos verificados:*

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.

3. Clique no botão **Configurações** à direita da janela.

4. Na janela que é aberta, na guia **Geral**, na seção **Tipos de arquivos**, selecione as configurações desejadas.

ALTERANDO E RESTAURANDO O NÍVEL DE SEGURANÇA

Dependendo das suas necessidades reais, você pode selecionar um dos níveis predefinidos de segurança de arquivos/da memória ou configurar você mesmo o Antivírus de Arquivos.

Ao configurar o Antivírus de Arquivos, você pode reverter as configurações recomendadas a qualquer momento. Essas configurações são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

- *Para alterar o nível de segurança atual dos arquivos e da memória:*

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.

3. À direita da janela, na seção **Nível de segurança**, defina o nível de segurança necessário ou clique no botão **Configurações** para modificar as configurações manualmente.

> Se você modificar as configurações manualmente, o nome do nível de segurança será alterado para **Personalizado**.

- *Para restaurar as configurações de proteção padrão:*

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.

3. Clique no botão **Nível padrão** na seção **Nível de segurança** à direita da janela.

SELECIONANDO O MODO DE VERIFICAÇÃO

O modo de verificação é a condição que aciona a atividade do Antivírus de Arquivos. A configuração padrão do Kaspersky Anti-Virus é o modo inteligente, que determina se o objeto deve ser verificado de acordo com as ações executadas com ele. Por exemplo, ao trabalhar com um documento do Microsoft Office, o Kaspersky Anti-Virus verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação.

Você pode alterar o modo de verificação dos objetos. O modo de verificação deve ser selecionado de acordo com os arquivos com os quais você trabalha na maior parte do tempo.

Para alterar o modo de verificação dos objetos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.
4. Na janela que é aberta, na guia **Adicional**, na seção **Modo de verificação**, selecione o modo desejado.

USANDO A ANÁLISE HEURÍSTICA

Durante a operação do Antivírus de Arquivos, a *análise de assinaturas* é usada sempre: O Kaspersky Anti-Virus compara o objeto encontrado com os registros do banco de dados.

Para melhorar a eficiência da proteção, você pode usar a *análise heurística* (ou seja, a análise da atividade que um objeto executa no sistema). Essa análise permite detectar novos objetos maliciosos que ainda não estão descritos nos bancos de dados.

Para ativar a análise heurística:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.
4. Na janela que é aberta, na guia **Desempenho**, na seção **Métodos de verificação**, marque a caixa **Análise heurística** e especifique o nível de detalhamento da verificação.

SELECIONANDO A TECNOLOGIA DE VERIFICAÇÃO

Além da análise heurística, você pode usar tecnologias especiais que permitem aumentar a velocidade da verificação de vírus através da exclusão dos arquivos que não foram modificados desde sua última verificação.

Para ativar as tecnologias de verificação de objetos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.
4. Na janela que é aberta, na guia **Adicional**, na seção **Tecnologias de verificação**, selecione os valores desejados.

ALTERANDO AS AÇÕES A SEREM EXECUTADAS COM OS OBJETOS DETECTADOS

Quando são detectados objetos infectados ou possivelmente infectados, o aplicativo executa a ação especificada.

Para alterar a ação a ser executada com os objetos detectados especificada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.

3. À direita da janela, na seção **Ação ao detectar ameaça**, selecione a opção desejada.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS

Um método comum para ocultar vírus é incorporá-los em arquivos compostos, como arquivos comprimidos, bancos de dados, etc. Para detectar vírus que estão ocultos dessa forma, é necessário descompactar os arquivos compostos, o que pode reduzir significativamente a velocidade da verificação.

Para cada tipo de arquivo composto, você pode selecionar a verificação de todos os arquivos ou apenas dos arquivos novos. Para selecionar, clique no link ao lado do nome do objeto. Seu valor é mudado quando você clica nele. Se você selecionar o modo de verificação apenas de arquivos novos e modificados (veja a página 96), não poderá selecionar os links que permitem verificar todos os arquivos ou apenas os arquivos novos.

Por padrão, o Kaspersky Anti-Virus verifica apenas os objetos OLE incorporados.

Ao verificar arquivos compostos grandes, sua descompactação preliminar pode levar muito tempo. É possível reduzir esse período ativando a descompactação de arquivos compostos em background quando eles excederem o tamanho de arquivo especificado. Se for detectado um objeto malicioso enquanto você trabalha com esse arquivo, o Kaspersky Anti-Virus o notificará.

Você pode limitar o tamanho máximo do arquivo composto verificado. Os arquivos compostos maiores que o tamanho especificado não serão verificados.

Quando arquivos grandes são extraídos de arquivos comprimidos, eles são verificados mesmo que a caixa **Não descompactar arquivos compostos grandes** esteja marcada.

- *Para modificar a lista de arquivos compostos verificados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.
  4. Na janela que é aberta, na guia **Desempenho**, na seção **Verificação de arquivos compostos**, selecione os tipos de arquivos compostos que devem ser verificados.

- *Para definir o tamanho máximo dos arquivos compostos a serem verificados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.
  4. Na janela que é aberta, na guia **Desempenho**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.
  5. Na janela **Arquivos compostos**, marque a caixa **Não descompactar arquivos compostos grandes** e especifique o tamanho máximo de arquivo.

- *Para descompactar arquivos compostos grandes em background:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Clique no botão **Configurações** na seção **Nível de segurança** à direita da janela.

4. Na janela que é aberta, na guia **Desempenho**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.

5. Na janela **Arquivos compostos**, marque a caixa **Extrair arquivos compostos em background** e especifique o tamanho mínimo de arquivo.

OTIMIZAÇÃO DA VERIFICAÇÃO

Você pode reduzir o tempo de verificação e aumentar a velocidade do Kaspersky Anti-Virus. Isso é possível verificando apenas os arquivos novos e aqueles que foram alterados desde a última vez que foram verificados. Esse modo se aplica a arquivos simples e compostos.

➧ *Para verificar somente arquivos novos e alterados:*

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.

3. Clique no botão **Configurações** à direita da janela.

4. Na janela que é aberta, na guia **Desempenho**, na seção **Otimização da verificação**, marque a caixa **Verificar somente arquivos novos e alterados**.

ANTIVÍRUS DE EMAIL

O *Antivírus de Email* verifica as mensagens enviadas e recebidas quanto à presença de objetos maliciosos. Ele abre ao iniciar o sistema operacional, sendo executado continuamente, verificando todos os emails enviados ou recebidos através dos protocolos POP3, SMTP, IMAP, MAPI e NNTP, além das conexões criptografadas (SSL) por POP3 e IMAP (consulte a seção "Verificando conexões criptografadas" na página 114).

O indicador de operação do componente é o ícone do aplicativo na área de notificação da barra de tarefas, que tem a seguinte aparência sempre que um email é verificado.

Você pode especificar os tipos de mensagens que devem ser verificados e selecionar o nível de segurança (veja a página 98) (configurações que afetam a profundidade da verificação).

O aplicativo intercepta todas as mensagens enviadas ou recebidas pelo usuário e analisa seus componente básicos: cabeçalho, corpo e anexos. O corpo e os anexos da mensagem (inclusive os objetos OLE anexos) são verificados quanto à presença de ameaças.

Por padrão, o modo de uso de registros dos bancos de dados do aplicativo para procurar ameaças está sempre ativado. Além disso, você pode ativar a análise heurística. E pode ativar a filtragem de anexos (veja a página 99), que permite renomear ou excluir automaticamente determinados tipos de arquivos.

Se for detectada uma ameaça, o Kaspersky Anti-Virus atribuirá um dos seguintes status ao objeto encontrado:

- programa malicioso (como um *vírus* ou um *cavalo de Troia*);

- *possivelmente infectado* (suspeito), quando a verificação não puder determinar se o objeto está infectado ou não. O arquivo pode conter uma sequência de código adequada aos vírus ou o código modificado de um vírus conhecido.

O aplicativo bloqueia a mensagem, exibe uma notificação sobre a ameaça detectada e executa a ação atribuída. É possível alterar as ações a serem executadas com uma ameaça detectada (consulte a seção "Alterando as ações a serem executadas com os objetos detectados" na página 99).

Se estiver trabalhando no modo automático (consulte a seção "Selecionando o modo de proteção" na página 77), o Kaspersky Anti-Virus aplicará automaticamente a ação recomendada pelos especialistas da Kaspersky Lab ao detectar objetos perigosos. Para objetos maliciosos, a ação é **Desinfetar. Excluir se a desinfecção falhar** e, para objetos suspeitos, é **Mover para a Quarentena**.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup para posterior restauração ou desinfecção. Os objetos suspeitos (possivelmente infectados) são colocados em quarentena. Você pode ativar a verificação de objetos em quarentena após cada atualização.

Depois de ser desinfetado, o email é disponibilizado novamente ao usuário. Se a desinfecção falhar, o objeto infectado será excluído da mensagem. Depois da verificação de vírus, um texto especial é inserido na linha de assunto do email, informando que ele foi processado pelo Kaspersky Anti-Virus.

É fornecido um plug-in integrado para o Microsoft Office Outlook (consulte a seção "Verificação de email no Microsoft Office Outlook" na página 100) que permite ajustar o programa de email.

Se você usa o The Bat!, o Kaspersky Anti-Virus poderá ser usado em conjunto com outros aplicativos antivírus. Nesse caso, as regras de processamento do tráfego de email (consulte a seção "Verificação de email no The Bat!" na página 100) são configuradas diretamente no The Bat! e substituem as configurações de proteção de email do aplicativo.

Ao trabalhar com outros programas de email, incluindo o Microsoft Outlook Express/Windows Mail, o Mozilla Thunderbird, o Eudora e o Incredimail, o componente Antivírus de Email verifica os emails dos protocolos SMTP, POP3, IMAP e NNTP.

Ao trabalhar com o programa de email Thunderbird, as mensagens transferidas por IMAP não serão verificadas quanto à presença de vírus se forem usados filtros que movem as mensagens da pasta **Caixa de entrada**.

NESTA SEÇÃO:

Ativando e desativando o Antivírus de Email 97

Criando um escopo de proteção 98

Alterando e restaurando o nível de segurança 98

Usando a análise heurística 99

Alterando as ações a serem executadas com os objetos detectados 99

Filtragem de anexos 99

Verificação de arquivos compostos 100

Verificação de email no Microsoft Office Outlook 100

Verificação de email no The Bat! 100

ATIVANDO E DESATIVANDO O ANTIVÍRUS DE EMAIL

Por padrão, o Antivírus de Email está ativado, funcionando no modo normal. Se necessário, você pode desativar o Antivírus de Email.

Para desativar o Antivírus de Email:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.

3. À direita da janela, desmarque a caixa **Ativar Antivírus de Email**.

CRIANDO UM ESCOPO DE PROTEÇÃO

O escopo de proteção consiste no tipo de mensagens a serem verificadas. Por padrão, o Kaspersky Anti-Virus verifica os emails enviados e recebidos.

Se você optou por verificar apenas as mensagens recebidas, é recomendável verificar as mensagens enviadas ao começar a usar o Kaspersky Anti-Virus, pois é provável que existam no computador worms que se distribuem por email. Isso evitará situações desagradáveis geradas pelo envio em massa de emails infectados sem monitoramento do seu computador.

O escopo de proteção também inclui as configurações usadas para integrar o componente Antivírus de Email ao sistema e os protocolos a serem verificados. Por padrão, o componente Antivírus de Email é integrado aos programas de email Microsoft Office Outlook e The Bat!

Para desativar a verificação de emails enviados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Use a guia **General** da janela exibida para selecionar, na seção **Escopo de proteção**, a opção **Apenas mensagens enviadas**.

Para selecionar os protocolos que devem ser verificados e as configurações para integrar o Antivírus de Email ao sistema:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela que é aberta, na guia **Adicional**, na seção **Conectividade**, selecione as configurações desejadas.

ALTERANDO E RESTAURANDO O NÍVEL DE SEGURANÇA

Dependendo das suas necessidades reais, você pode selecionar um dos níveis predefinidos de segurança de emails ou configurar você mesmo o Antivírus de Email.

A Kaspersky Lab recomenda não configurar o Antivírus de Email sozinho. Na maioria dos casos, basta selecionar outro nível de segurança.

Ao configurar o Antivírus de Email, você pode reverter os valores recomendados a qualquer momento. Essas configurações são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

Para alterar o nível de segurança de email predefinido:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. À direita da janela, na seção **Nível de segurança**, defina o nível de segurança necessário ou clique no botão **Configurações** para modificar as configurações manualmente.

Se você modificar as configurações manualmente, o nome do nível de segurança será alterado para **Personalizado**.

- *Para restaurar as configurações de proteção de email padrão:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Nível padrão** na seção **Nível de segurança** à direita da janela.

USANDO A ANÁLISE HEURÍSTICA

Durante o funcionamento do Antivírus de Email, a *análise de assinaturas* é usada sempre: O Kaspersky Anti-Virus compara o objeto encontrado com os registros do banco de dados.

Para melhorar a eficiência da proteção, você pode usar a *análise heurística* (ou seja, a análise da atividade que um objeto executa no sistema). Essa análise permite detectar novos objetos maliciosos que ainda não estão descritos nos bancos de dados.

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela que é aberta, na guia **Geral**, na seção **Métodos de verificação**, marque a caixa **Análise heurística** e especifique o nível de detalhamento da verificação.

ALTERANDO AS AÇÕES A SEREM EXECUTADAS COM OS OBJETOS DETECTADOS

Quando são detectados objetos infectados ou possivelmente infectados, o aplicativo executa a ação especificada.

- *Para alterar a ação a ser executada com os objetos detectados especificada:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. À direita da janela, na seção **Ação ao detectar ameaça**, selecione a opção desejada.

FILTRAGEM DE ANEXOS

Os malwares são distribuídos com mais frequência em emails, como objetos anexados às mensagens. Para proteger o computador, por exemplo, da execução automática de arquivos anexos, é possível ativar a filtragem de anexos, que pode renomear ou excluir automaticamente arquivos de determinados tipos.

- *Para ativar a filtragem de anexos:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.

4. Use a guia **Filtro de anexos** na janela exibida para selecionar o modo de filtragem dos anexos. Ao selecionar qualquer dos dois últimos modos, a lista de tipos de arquivos (extensões) será ativada e nela você poderá selecionar os tipos desejados ou adicionar uma máscara para selecionar um novo tipo.

   Para adicionar uma nova máscara à lista, clique no link **Adicionar** para abrir a janela **Inserir máscara de nomes de arquivos** e inserir as informações desejadas.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS

Um método comum para ocultar vírus é incorporá-los em arquivos compostos, como arquivos comprimidos, bancos de dados, etc. Para detectar vírus que estão ocultos dessa forma, é necessário descompactar os arquivos compostos, o que pode reduzir significativamente a velocidade da verificação.

Você pode ativar ou desativar a verificação de arquivos comprimidos anexados e limitar o tamanho máximo dos arquivos comprimidos a serem verificados.

Se o computador não estiver protegido por nenhum software de rede local (o acesso à Internet for direto, sem um servidor proxy ou um firewall), é recomendável não desativar a verificação de arquivos comprimidos anexos.

Para configurar a verificação de arquivos compostos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Use a guia **Geral** na janela exibida para definir as configurações desejadas.

VERIFICAÇÃO DE EMAIL NO MICROSOFT OFFICE OUTLOOK

Se você usa o Microsoft Office Outlook como programa de email, é possível modificar outras configurações para a verificação de vírus em seus emails.

Ao instalar o Kaspersky Anti-Virus, um plug-in especial é instalado no Microsoft Office Outlook. Ele permite configurar rapidamente o Antivírus de Email, além de determinar quando os emails serão verificados quanto à presença de objetos perigosos.

O plug-in é fornecido como uma guia **Proteção de email** localizada no menu **Ferramentas → Opções**.

Para definir o tempo adequado para a verificação de email:

1. Abra a janela principal do aplicativo Microsoft Outlook.
2. Selecione **Ferramentas → Opções** no menu do aplicativo.
3. Use a guia **Proteção de email** para selecionar as configurações desejadas.

VERIFICAÇÃO DE EMAIL NO THE BAT!

As ações referentes a objetos de email infectados no The Bat! são definidas usando as ferramentas do próprio aplicativo.

As configurações do Antivírus de Email que determinam se as mensagens enviadas e recebidas devem ser verificadas, quais ações devem ser executadas com objetos perigosos em emails e quais exclusões devem ser aplicadas são ignoradas. A única opção que o The Bat! considera é a verificação de arquivos comprimidos anexos.

As configurações da proteção de email se estendem a todos os componentes antivírus instalados no computador compatíveis com o The Bat!

Os emails recebidos são verificados primeiro pelo Antivírus de Email e somente depois pelo plug-in do The Bat! Se um objeto malicioso for detectado, você receberá uma notificação do Kaspersky Anti-Virus. Se você selecionar a ação **Desinfetar** (**Excluir**) na janela de notificações do Antivírus de Email, as ações para eliminar a ameaça serão executadas pelo Antivírus de Email. Se você selecionar a ação **Ignorar** na janela de notificações, o objeto será desinfetado pelo plug-in do The Bat! Ao enviar mensagens de email, a verificação é executada primeiro pelo plug-in e depois pelo Antivírus de Email.

Você deve definir os seguintes critérios:

- os fluxos de email (enviados, recebidos) que devem ser verificados;
- em que momento os objetos de email devem ser verificados (ao abrir um a mensagem, ou antes de salvá-la no disco);
- as ações que são executadas pelo programa de email caso sejam detectados objetos perigosos nos emails. Por exemplo, você pode selecionar:
  - **Attempt to disinfect infected parts** – se esta opção estiver selecionada, será feita uma tentativa de desinfetar o objeto infectado e, se isso não for possível, ele permanecerá na mensagem.
  - **Delete infected parts** – se esta opção estiver selecionada, o objeto perigoso na mensagem será excluído, independentemente de ele estar infectado ou de haver uma suspeita de que esteja infectado.

Por padrão, o The Bat! coloca todos os objetos de email infectados na Quarentena sem tentar desinfetá-los.

O The Bat! não inclui cabeçalhos específicos nos emails que contêm objetos perigosos.

➧ *Para configurar as regras de proteção de email no The Bat! :*

1. Abra a janela principal do The Bat!.
2. Selecione o item **Settings** no menu **Properties** do programa de email.
3. Selecione o objeto **Virus protection** na árvore de configurações.

ANTIVÍRUS DA WEB

Sempre que você usa a Internet, as informações armazenadas no computador correm o risco de ser infectadas por programas perigosos. Eles podem se infiltrar no computador enquanto você baixa algum software gratuito ou navega por sites sabidamente seguros e que sofreram ataques de hackers antes de você visitá-los. Além disso, os worms de rede podem invadir seu computador sem que você abra uma página da Web ou baixe um arquivo, simplesmente por seu computador estar conectado à Internet.

O componente *Antivírus da Web* foi criado para garantir a segurança ao usar a Internet. Ele protege o computador contra dados recebidos pelos protocolos HTTP, HTTPS e FTP, e também evita a execução de scripts perigosos no computador.

A proteção da Web monitora somente o fluxo de dados que passa pelas portas incluídas na lista de portas monitoradas. Uma lista das portas mais usadas para a transferência de dados é incluída no kit de distribuição do Kaspersky Anti-Virus. Se você usar portas que não estão nessa lista, adicione-as à lista de portas monitoradas (consulte a seção "Criando uma lista de portas monitoradas" na página 117) para garantir a proteção dos fluxos de dados direcionados por elas.

Um conjunto de configurações chamado nível de segurança define como o fluxo de dados será verificado (consulte a seção "Selecionando o nível de segurança do Antivírus da Web" na página 103). Se o Antivírus da Web detectar uma ameaça, ele executará a ação atribuída.

A Kaspersky Lab recomenda não configurar o Antivírus da Web sozinho. Na maioria dos casos, basta selecionar o nível de segurança apropriado.

Algoritmo de operação do componente

O Antivírus da Web protege os dados que chegam ao computador e são transferidos dele através de HTTP, HTTPS e FTP, e evita que scripts perigosos sejam executados no computador. Por padrão, a verificação de conexões seguras (via HTTPS) está desativada; você pode ativá-la e configurá-la (consulte a seção "Verificando conexões criptografadas" na página 114).

Os dados são protegidos usando o seguinte algoritmo:

1. Cada página da Web ou arquivo que é acessado pelo usuário ou por um aplicativo através dos protocolos HTTP, HTTPS ou FTP é interceptado e analisado pelo Antivírus da Web quanto à presença de código malicioso. Os objetos maliciosos são detectados usando os bancos de dados e o algoritmo heurístico do Kaspersky Anti-Virus. O banco de dados contém descrições de todos os programas maliciosos conhecidos até o momento e os métodos para neutralizá-los. O algoritmo heurístico pode detectar novos vírus que ainda não foram inseridos no banco de dados.

2. Após a análise, estarão disponíveis as seguintes ações:

   - Se uma página da Web ou um objeto acessado pelo usuário contiver código malicioso, seu acesso será bloqueado. Será exibida uma notificação de que o objeto ou a página solicitada está infectado.

   - Se o arquivo ou a página da Web não contiver código malicioso, o programa concederá acesso a ele imediatamente.

Os scripts são verificados de acordo com o seguinte algoritmo:

1. Cada script executado é interceptado pelo Antivírus da Web e analisado quanto à presença de código malicioso.

2. Se o script contiver código malicioso, o Antivírus da Web o bloqueará e informará ao usuário através de uma mensagem pop-up especial.

3. Se nenhum código malicioso for descoberto no script, ele será executado.

O Antivírus da Web intercepta somente os scripts que usam a funcionalidade do Microsoft Windows Script Host.

NESTA SEÇÃO:

Ativando e desativando o Antivírus da Web 103

Selecionando o nível de segurança do Antivírus da Web 103

Alterando as ações a serem executadas com objetos perigosos 104

Verificando URLs usando os bancos de dados de endereços suspeitos e de phishing 104

Usando a análise heurística 105

Bloqueando scripts perigosos 105

Otimização da verificação 106

Consultor de URLs Kaspersky 106

Criando uma lista de endereços confiáveis 107

Restaurando as configurações padrão do Antivírus da Web 108

ATIVANDO E DESATIVANDO O ANTIVÍRUS DA WEB

Existem duas formas de ativar ou desativar o componente:

- na janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44);
- na janela de configurações (consulte a seção "Janela de configurações do aplicativo" na página 48).

Para ativar ou desativar o Antivírus da Web na janela principal:

1. Abra a janela principal do aplicativo e selecione a seção **Centro de Proteção** à esquerda da janela.
2. À direita da janela, clique para abrir as seções **Segurança Online** ou **Proteção do Sistema e de Aplicativos**.
3. Abra o menu para selecionar uma ação do componente clicando no botão **Antivírus da Web** e selecionando **Ativar Antivírus da Web** ou **Desativar Antivírus da Web**.

   Ao ativar um componente, o ícone à sua esquerda fica verde; ao desativá-lo, o ícone fica cinza.

Para ativar ou desativar o Antivírus da Web na janela de configurações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. À direita da janela, marque a caixa **Ativar Antivírus da Web** para ativar esse componente. Desmarque a caixa para desativar o componente.

SELECIONANDO O NÍVEL DE SEGURANÇA DO ANTIVÍRUS DA WEB

O nível de segurança é estabelecido como uma configuração predefinida do Antivírus da Web que fornece um determinado nível de proteção para os dados recebidos e transmitidos via HTTP, HTTPS e FTP. Os especialistas da Kaspersky Lab diferenciam três níveis de segurança:

- O nível Alto oferece a proteção máxima, necessária ao trabalhar em um ambiente perigoso.

- O nível Recomendado oferece a proteção ideal, recomendada na maioria dos casos.
- O nível Baixo permite o desempenho máximo.

O usuário deve decidir o nível a ser selecionado de acordo com suas condições de trabalho e sua situação atual.

Para selecionar um dos níveis de segurança predefinidos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Use o controle deslizante à direita da janela para fechar o nível de segurança desejado.

Se nenhum dos níveis predefinidos atender aos seus requisitos, você poderá configurar o Antivírus da Web, por exemplo, modificando o nível de profundidade da verificação durante a análise heurística. Essa configuração mudará o nome do nível de segurança para **Personalizado**.

Se for necessário reverter novamente para um nível de segurança predefinido, basta restaurar a configuração padrão do componente (consulte a seção "Restaurando as configurações padrão do Antivírus da Web" na página 108).

ALTERANDO AS AÇÕES A SEREM EXECUTADAS COM OBJETOS PERIGOSOS

Quando a análise de um objeto do tráfego da Web mostrar que ele contém código malicioso, a resposta do componente Antivírus da Web dependerá da ação selecionada.

O Antivírus da Web sempre bloqueia ações de scripts perigosos e emite mensagens que informam o usuário sobre a ação executada. A ação com um script perigoso não pode ser alterada; a única modificação disponível é desativar o módulo de verificação de scripts (consulte a seção "Bloqueando scripts perigosos" na página 105).

Ao trabalhar no modo automático, o Kaspersky Anti-Virus aplica automaticamente a ação recomendada pelos especialistas da Kaspersky Lab ao detectar objetos perigosos.

Para selecionar a ação a ser executada com os objetos detectados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Na seção **Ação ao detectar ameaça** à direita da janela, escolha a ação que o aplicativo deve executar com o objeto perigoso descoberto.

VERIFICANDO URLS USANDO OS BANCOS DE DADOS DE ENDEREÇOS SUSPEITOS E DE PHISHING

O Antivírus da Web verifica o tráfego da Web quanto à presença de vírus e também verifica se os URLs estão nas listas de endereços suspeitos ou de phishing.

Ao verificar se os links estão incluídos na lista de endereços de phishing permite evitar ataques de phishing que parecem com mensagens de email de supostas instituições financeiras e contêm links para os sites dessas organizações. O texto da mensagem convence o leitor a clicar no link e a inserir informações confidenciais na janela que se segue, como um número de cartão de crédito ou o logon e a senha de um site de banco virtual na Internet, no qual podem ser realizadas operações financeiras. Um ataque de phishing pode ser disfarçado, por exemplo, como uma carta de seu banco com um link para o site oficial da instituição. Ao clicar no link, você é direcionado para uma cópia exata do site do banco e pode até ver o endereço real no navegador, embora, na verdade, esteja em um site falso. Desse momento em diante, todas as suas ações no site são rastreadas e podem ser usadas para roubá-lo.

As listas de URLs de phishing estão incluídas no kit de distribuição do Kaspersky Anti-Virus. Como os links para sites de phishing podem ser recebidos de outras fontes além dos emails, como mensagens do ICQ, o Antivírus da Web monitora as tentativas de acessar um site de phishing no nível do tráfego da Web e bloqueia o acesso a esses locais.

Para configurar o Antivírus da Web para verificar os URLs incluídos nos bancos de dados de URLs suspeitos e de phishing:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Na seção **Métodos de verificação** da guia **Geral**, verifique se as caixas **Verificar se os URLs estão listados no banco de dados de URLs suspeitos** e **Verificar se os URLs estão listados no banco de dados de URLs de phishing** estão selecionadas.

USANDO A ANÁLISE HEURÍSTICA

A *Análise heurística* é um método de inspeção especial. É usado para analisar a atividade de um objeto no sistema host. Se essa atividade for característica de objetos perigosos, o objeto será reconhecido com probabilidade suficiente como malicioso ou suspeito, mesmo que o código perigosos contido nele ainda seja desconhecido dos analistas de vírus.

Você pode selecionar o nível de profundidade da análise heurística:

- verificação leve – uma verificação rápida;
- verificação profunda – uma verificação completa que leva mais tempo;
- verificação média – uma combinação ideal de velocidade e profundidade de verificação, adequada na maioria dos casos.

Se a análise heurística revelar um objeto malicioso, o Kaspersky Anti-Virus o notificará sobre isso e sugerirá o tratamento apropriado para o objeto detectado.

A análise heurística está ativada por padrão, com o nível de profundidade definido como **verificação média**.

Para ativar a análise heurística e definir seu nível de profundidade ou desativá-la:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Para ativar a análise heurística, vá para a guia **Geral** e, na seção **Métodos de verificação**, marque a caixa **Análise heurística**. Use o controle deslizante abaixo para definir o nível de profundida de da verificação desejado. Desmarque a caixa **Análise Heurística** para não usar esse método de verificação.

BLOQUEANDO SCRIPTS PERIGOSOS

O Antivírus da Web pode verificar todos os scripts processados no Microsoft Internet Explorer e também todos os outros scripts WSH (Java, Visual Basic Script, etc.) executados enquanto o usuário trabalha no computador. Se um script representar uma ameaça para o computador, ele será bloqueado.

Para que o Antivírus da Web verifique e bloqueie os scripts:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Confirme se a caixa **Bloquear scripts perigosos no Microsoft Internet Explorer** está marcada na guia **Geral** da seção **Adicional**.

OTIMIZAÇÃO DA VERIFICAÇÃO

Para detectar códigos maliciosos de forma mais eficiente, o Antivírus da Web armazena em cache fragmentos dos objetos baixados da Internet. Com esse método, o Antivírus da Web verifica um objeto somente depois de seu download completo. Então, o objeto é verificado quanto à presença de vírus e devolvido ao usuário ou bloqueado, dependendo dos resultados da verificação.

O armazenamento dos objetos em cache aumenta seu tempo de processamento e, portanto, o tempo para o aplicativo retorná-los ao usuário. O armazenamento em cache pode gerar problemas ao baixar ou processar objetos grandes, pois a conexão com o cliente HTTP pode atingir o tempo limite.

Para solucionar esse problema, é recomendável limitar o tempo de armazenamento em cache dos fragmentos de objetos baixados da Internet. Quando o período especificado expirar, o usuário receberá a parte do objeto baixada sem verificação e, quando o objeto for totalmente copiado, ele será verificado integralmente. Assim, é possível reduzir o tempo necessário para transferir o objeto para o usuário e eliminar o problema de desconexão. Nesse caso, o nível de segurança de Internet não será reduzido.

A remoção do limite de tempo de cache resulta na maior eficiência da verificação antivírus, tornando porém o acesso ao objeto um pouco mais lento.

Para definir um limite de tempo para o armazenamento de fragmentos em buffer ou para removê-lo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Para limitar a duração da verificação do tráfego, na guia **Geral**, na seção **Adicional**, marque a caixa **Limitar tempo de armazenamento do tráfego em cache para otimizar a verificação**. Se desejar cancelar a restrição, desmarque a caixa.

CONSULTOR DE URLS KASPERSKY

O Kaspersky Anti-Virus inclui o módulo de verificação de URLs gerenciado pelo Antivírus da Web. Esse módulo é incorporado nos navegadores Microsoft Internet Explorer e Mozilla Firefox como um plug-in.

Esse módulo verifica se os links localizados na página da Web pertencem à lista de endereços suspeitos ou de phishing. Você pode criar uma lista de endereços cujo conteúdo não será verificado quanto à presença de URLs suspeitos ou de phishing, ou uma lista de sites cujo conteúdo deve ser verificado. Você também pode excluir completamente a verificação de URLs.

As opções de configuração do Consultor de URLs Kaspersky listadas a seguir podem ser selecionadas na janela de configurações do aplicativo e também na janela de configurações do módulo consultor que é aberto no navegador da Web.

- *Para criar uma lista de sites cujo conteúdo não será verificado quanto à presença de URLs suspeitos ou de phishing:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. Clique no botão **Configurações** à direita da janela.

     A janela **Antivírus da Web** é aberta.
  4. Na guia **Navegação Segura** da seção **Consultor de URLs Kaspersky**, selecione **Em todas as páginas da Web, exceto as exclusões** e clique no botão **Exclusões**.
  5. Use a janela **Exclusões** que é exibida para criar a lista de sites cujo conteúdo não será verificado quanto à presença de URLs suspeitos ou de phishing.

- *Para criar uma lista de sites cujo conteúdo deve ser verificado quanto à presença de URLs suspeitos ou de phishing:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. Clique no botão **Configurações** à direita da janela.

     A janela **Antivírus da Web** é aberta.
  4. Na guia **Navegação Segura** da seção **Consultor de URLs Kaspersky**, selecione **Nas páginas da Web selecionadas** e clique no botão **Selecionar**.
  5. Use a janela **URLs verificados** que é exibida para criar a lista de endereços da Web cujo conteúdo será verificado quanto à presença de URLs suspeitos ou de phishing.

- *Se desejar que nenhum URLs seja verificado pelo consultor:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. Clique no botão **Configurações** à direita da janela.

     A janela **Antivírus da Web** é aberta.
  4. Na guia **Navegação Segura**, na seção **Consultor de URLs Kaspersky**, marque a caixa **Verificar URLs**.

- *Para abrir a janela de configurações do Consultor de URLs Kaspersky no navegador da Web,*

  clique no botão com o ícone do Kaspersky Anti-Virus na barra de ferramentas do navegador.

CRIANDO UMA LISTA DE ENDEREÇOS CONFIÁVEIS

É possível criar uma lista de endereços da Web em cujo conteúdo você confia incondicionalmente. O Antivírus da Web não analisará os dados desses endereços quanto à presença de objetos perigosos. Esta opção pode ser útil, por exemplo, quando o Antivírus da Web interferir no download de um arquivo específico de um site conhecido.

Para criar a lista de endereços confiáveis:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Na guia **URLs confiáveis**, marque a caixa **Não verificar o tráfego da Web de URLs confiáveis** e crie a lista de URLs que oferecem conteúdo confiável.

Se você precisar excluir temporariamente um endereço da lista confiável, não será necessário excluí-lo; desmarcar a caixa correspondente à esquerda terá o efeito desejado.

RESTAURANDO AS CONFIGURAÇÕES PADRÃO DO ANTIVÍRUS DA WEB

Se você não estiver satisfeito com o comportamento do Antivírus da Web configurado, poderá restaurar a configuração do componente recomendada pela Kaspersky Lab. Essas configurações estão reunidas no nível de segurança **Recomendado**.

Para restaurar as configurações padrão do Antivírus da Web:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Nível padrão** na seção **Nível de segurança** à direita da janela.

   O nível de segurança será definido como **Recomendado**.

ANTIVÍRUS DE IM

O Antivírus de IM verifica o tráfego de mensagens instantâneas (os chamados *mensageiros da Internet*).

As mensagens instantâneas podem conter links para sites suspeitos e para sites deliberadamente usados por hackers em ataques de phishing. Programas maliciosos usam programas de IM para enviar spam e links para os programas (ou os próprios programas), que roubam números de ID e senhas dos usuários.

O Kaspersky Anti-Virus garante a operação segura de vários aplicativos de mensagens instantâneas, incluindo ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent e IRC.

Alguns programas de IM, como Yahoo! Messenger e Google Talk, usam conexões seguras. Para verificar o tráfego gerado por esses programas, é necessário ativar a verificação de conexões seguras (veja a página 114).

O Antivírus de IM intercepta as mensagens e as verifica quanto à presença de objetos ou URLs perigosos. Você pode selecionar os tipos de mensagens (veja a página 109) que devem ser verificadas e vários métodos de verificação.

Se forem detectadas ameaças em uma mensagem, o Antivírus de IM substitui a mensagem por um aviso para o usuário.

Os arquivos transferidos pelos programas de mensagens instantâneas são verificados pelo componente Antivírus de Arquivos quando ocorrem tentativas de salvá-los.

NESTA SEÇÃO:

Ativando e desativando o Antivírus de IM 109

Criando um escopo de proteção 109

Selecionando o método de verificação..... 109

ATIVANDO E DESATIVANDO O ANTIVÍRUS DE IM

Por padrão, o Antivírus de IM está ativado, funcionando no modo normal. Se necessário, você pode desativar o Antivírus de IM.

Para desativar o Antivírus de IM:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, desmarque a caixa **Ativar Antivírus de IM**.

CRIANDO UM ESCOPO DE PROTEÇÃO

O escopo de proteção consiste no tipo de mensagens a serem verificadas. Por padrão, o Kaspersky Anti-Virus verifica os emails enviados e recebidos. Se tiver certeza de que as mensagens enviadas por você não contêm objetos perigosos, você pode desativar a verificação do tráfego de saída.

Para desativar a verificação de mensagens enviadas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, na seção **Escopo de proteção**, selecione a opção **Apenas mensagens recebidas**.

SELECIONANDO O MÉTODO DE VERIFICAÇÃO

Os métodos de verificação consistem em verificar se os URLs nas mensagens instantâneas estão incluídos na lista de endereços suspeitos e/ou na lista de endereços de phishing.

Para melhorar a eficiência da proteção, você pode usar a *análise heurística* (ou seja, a análise da atividade que um objeto executa no sistema). Essa análise permite detectar novos objetos maliciosos que ainda não estão descritos nos bancos de dados. Ao usar a análise heurística, todos os scripts incluídos em mensagens instantâneas são executados em um ambiente protegido. Se as atividades do script forem típicas de objetos maliciosos, provavelmente o objeto será classificado como malicioso ou suspeito. Por padrão, a análise heurística está ativada.

Para verificar os links nas mensagens usando o banco de dados de endereços suspeitos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, na seção **Métodos de verificação**, marque a caixa **Verificar se os URLs estão listados no banco de dados de URLs suspeitos**.

- *Para verificar os links nas mensagens usando o banco de dados de endereços de phishing:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
  3. À direita da janela, na seção **Métodos de verificação**, marque a caixa **Verificar se os URLs estão listados no banco de dados de URLs de phishing**.

- *Para ativar a análise heurística:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
  3. À direita da janela, na seção **Métodos de verificação**, marque a caixa **Análise heurística** e defina o nível de detalhamento desejado.

DEFESA PROATIVA

A Defesa Proativa garante a proteção contra novas ameaças que ainda não foram incluídas nos bancos de dados do Kaspersky Anti-Virus.

As tecnologias preventivas fornecidas pela Defesa Proativa neutralizam novas ameaças antes que elas danifiquem o seu computador. Diferentemente das tecnologias responsivas, que analisam o código com base nos registros dos bancos de dados do Kaspersky Anti-Virus, as tecnologias preventivas reconhecem uma nova ameaça no computador por meio da sequência de ações executadas pelo programa. Se, como resultado da análise de atividades, a sequência de ações do aplicativo for considerada suspeita, o Kaspersky Anti-Virus bloqueará a atividade desse aplicativo.

Por exemplo, quando forem detectadas ações como o programa copiar a si mesmo em recursos de rede, na pasta de inicialização ou no Registro do sistema, é muito provável que se trate de um worm. As sequências de ações perigosas também incluem tentativas de modificar o arquivo HOSTS, a instalação oculta de drivers, etc. Você pode desativar o monitoramento (veja a página 111) de atividades perigosas ou editar as regras de monitoramento (veja a página 111).

Você pode criar um grupo de aplicativos confiáveis (veja a página 111) para a Defesa Proativa. Nesse caso, você não será notificado sobre as atividades desses aplicativos.

Se o computador executar o Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou o Microsoft Windows 7 x64, o controle não se aplicará a cada evento. Isso se deve a recursos específicos desses sistemas operacionais. Por exemplo, o controle não se aplicará rigidamente ao envio de dados por meio de aplicativos confiáveis e às atividades suspeitas do sistema.

NESTA SEÇÃO:

Ativando e desativando a Defesa Proativa 110

Criando um grupo de aplicativos confiáveis 111

Usando a lista de atividades perigosas 111

Alterando a regra de monitoramento de atividades perigosas 111

ATIVANDO E DESATIVANDO A DEFESA PROATIVA

Por padrão, a Defesa Proativa está ativada, funcionando no modo normal. Se necessário, você pode desativar a Defesa Proativa.

Para desativar a Defesa Proativa:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.
3. À direita da janela, desmarque a caixa **Ativar Defesa Proativa**.

CRIANDO UM GRUPO DE APLICATIVOS CONFIÁVEIS

Você pode criar um grupo de aplicativos confiáveis; a Defesa Proativa não monitorará sua atividade. Por padrão, a lista de aplicativos confiáveis inclui aplicativos com assinaturas digitais verificadas e aplicativos do banco de dados do Kaspersky Security Network.

Para alterar as configurações do grupo de aplicativos confiáveis:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.
3. À direita da janela, na seção **Aplicativos confiáveis**, marque as caixas ao lado das configurações desejadas.

USANDO A LISTA DE ATIVIDADES PERIGOSAS

Não é possível editar a lista de ações típicas de atividade perigosa. Você pode desativar o monitoramento de algumas atividades perigosas.

Para desativar o monitoramento de algumas atividades perigosas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela **Defesa Proativa** que é aberta, desmarque a caixa ao lado do tipo de atividade que você não deseja monitorar.

ALTERANDO A REGRA DE MONITORAMENTO DE ATIVIDADES PERIGOSAS

Não é possível editar as ações dos aplicativos classificadas com atividade perigosa. Você pode executar as seguintes ações:

- desativar o monitoramento de qualquer atividade (veja a página 111);
- criar uma lista de exclusões (veja a página 119) listando os aplicativos cujas atividades que você não considera perigosas;
- editar a regra usada pela Defesa Proativa ao detectar atividades perigosas;

Para editar a regra da Defesa Proativa:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.

3. Clique no botão **Configurações** à direita da janela.

4. Na janela **Defesa Proativa** que é aberta, na coluna **Evento**, selecione o evento cuja regra você deseja editar.

5. Configure o evento selecionado usando os links na seção **Descrição da regra**. Por exemplo:

   a. clique no link com a ação predefinida e, na janela **Selecionar ação** que é aberta, selecione a ação desejada;

   b. clique no link **Ativado/Desativado** para indicar se deve ser criado um relatório de execução da tarefa.

INSPETOR DO SISTEMA

O Inspetor do Sistema coleta dados sobre as ações de aplicativos no computador e fornece informações a outros componentes para aperfeiçoar a proteção.

Se a gravação de logs de atividade dos aplicativos estiver ativada, o Inspetor do Sistema permitirá reverter as ações executadas por programas maliciosos (veja a página 113). A reversão das ações após a detecção de alguma atividade maliciosa no sistema pode ser iniciada pelo componente Inspetor do Sistema com base nos padrões de atividades perigosas (consulte a seção "Usando padrões de atividades perigosas (BSS)" na página 113) ou pela Defesa Proativa e durante a execução de uma tarefa de verificação de vírus ou da operação do Antivírus de Arquivos (veja a página 90).

A resposta do componente à correspondência entre ações de aplicativos e padrões de atividades perigosas e a reversão das ações de programas maliciosos dependem do modo de operação do Kaspersky Anti-Virus.

Se forem detectadas ações suspeitas no sistema, os componentes de proteção do Kaspersky Anti-Virus podem solicitar informações adicionais do Monitor de atividades. Quando o Kaspersky Anti-Virus é executado no modo interativo, você pode exibir os dados de eventos coletados pelo componente Inspetor do Sistema em um relatório de atividades perigosas, o que ajuda a tomar decisões ao selecionar ações na janela de notificações. Quando o componente detecta um programa malicioso, o link para o relatório do Inspetor do Sistema é exibido na parte superior da janela de notificações (veja a página 152), perguntando o que fazer.

NESTA SEÇÃO:

Ativando e desativando o Inspetor do Sistema 112

Usando padrões de atividades perigosas (BSS) 113

Revertendo as ações de um programa malicioso 113

ATIVANDO E DESATIVANDO O INSPETOR DO SISTEMA

Por padrão, o Inspetor do Sistema está ativado e seu modo de execução depende do modo atual do Kaspersky Anti-Virus: automático ou interativo.

É recomendável não desativar o componente, exceto em casos de emergência, pois inevitavelmente isso afeta a eficiência da Defesa Proativa e a operação de outros componentes de proteção que podem solicitar os dados coletados pelo Monitor de atividades para identificar a possível ameaça detectada.

➧ *Para desativar o Inspetor do Sistema:*

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Inspetor do Sistema**.

3. À direita da janela, desmarque a caixa **Ativar Inspetor do Sistema**.

USANDO PADRÕES DE ATIVIDADES PERIGOSAS (BSS)

Os padrões de atividades perigosas (BSS – Behavior Stream Signatures) contêm sequências de ações típicas de aplicativos considerados perigosos. Se a atividade de um aplicativo corresponder a um padrão de atividades perigosas, o Kaspersky Anti-Virus executará a ação especificada.

Quando o Kaspersky Anti-Virus é atualizado, os padrões de atividades usados pelo Inspetor do Sistema são fornecidos de forma dinâmica com novas atividades para obter uma proteção atualizada e confiável.

Por padrão, quando o Kaspersky Anti-Virus é executado no modo automático, se a atividade de um aplicativo corresponder a um padrão de atividades perigosas, o Inspetor do Sistema moverá o aplicativo para a Quarentena. Ao ser executado no modo interativo (veja a página 77), o Inspetor do Sistema pergunta ao usuário o que fazer. Você pode especificar a ação que deve ser executada pelo componente quando a atividade de um aplicativo corresponder a um padrão de atividades perigosas.

Além da correspondência exata entre atividades de aplicativos e padrões de atividades perigosas, o Inspetor do Sistema também detecta ações que correspondem parcialmente a esses padrões e que são consideradas suspeitas com base na análise heurística. Se forem detectadas atividades suspeitas, o Inspetor do Sistema perguntará o que fazer independentemente do modo de operação.

- *Para selecionar a ação que deve ser executada pelo componente quando a atividade de um aplicativo corresponder a um padrão de atividades perigosas:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Inspetor do Sistema**.
3. À direita da janela, na seção **Análise heurística**, marque a caixa **Usar padrões atualizáveis de atividade perigosa (BSS)**.
4. Clique em **Selecionar ação** e especifique a ação desejada na lista suspensa.

REVERTENDO AS AÇÕES DE UM PROGRAMA MALICIOSO

Você pode usar o recurso do produto para reverter ações executadas por malware no sistema. Para permitir uma reversão, o Inspetor do Sistema deve registrar o histórico de atividades do programa.

Por padrão, o Kaspersky Anti-Virus reverte as ações automaticamente quando os componentes de proteção detectam atividade maliciosa. Ao ser executado no modo interativo (veja a página 77), o Inspetor do Sistema pergunta ao usuário o que fazer. Você pode especificar a operação que deve ser executada sempre que for detectada atividade maliciosa.

O procedimento de reverter operações de malware afeta um conjunto de dados definido rigidamente. Ele não tem consequências negativas para a integridade do sistema operacional ou dos dados no seu computador.

- *Para configurar a reversão de operações de malware:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Inspetor do Sistema**.
3. À direita da janela, na seção **Log de atividade de aplicativos**, marque a caixa **Salvar log de atividades**.
4. Clique em **Selecionar ação** e especifique a ação desejada na lista suspensa.

PROTEÇÃO DE REDE

Diversos componentes de proteção, ferramentas e configurações do Kaspersky Anti-Virus garantem em conjunto a segurança e o controle de suas atividades de rede.

As seções a seguir fornecem informações detalhadas a verificação de conexões seguras, das configurações do servidor proxy e do monitoramento de portas de rede.

NESTA SEÇÃO:

Verificação de conexões criptografadas 114

Configurando o servidor proxy 116

Criando uma lista de portas monitoradas 117

VERIFICAÇÃO DE CONEXÕES CRIPTOGRAFADAS

As conexões que usam os protocolos SSL/TSL protegem o canal de troca de dados na Internet. Os protocolos SSL/TSL permitem identificar as partes que trocam dados usando certificados eletrônicos, codificar os dados transferidos e assegurar sua integridade durante a transferência.

Esses recursos do protocolo são usados por hackers para disseminar programas maliciosos, pois a maioria dos aplicativos antivírus não verifica o tráfego SSL/TSL.

O Kaspersky Anti-Virus verifica as conexões criptografadas usando um certificado da Kaspersky Lab.

Se for detectado um certificado inválido ao conectar-se com o servidor (por exemplo, se o certificado for substituído por um invasor), será exibido uma notificação pop-up com a opção de aceitar ou rejeitar o certificado.

Se tiver certeza de que uma conexão com um site sempre é segura, apesar do certificado inválido, é possível adicionar o site à lista de URLs confiáveis (consulte a seção "Criando uma lista de endereços confiáveis" na página 107). O Kaspersky Anti-Virus não verificará mais a conexão criptografada com esse site.

Você pode usar o Assistente para Instalação de Certificados para instalar um certificado para verificar conexões criptografadas no modo semi-interativo no Microsoft Internet Explorer, no Mozilla Firefox (se ele não for executado) e no Google Chrome, além de obter instruções sobre como instalar o certificado da Kaspersky Lab para o Opera.

Para ativar a verificação de conexões criptografadas e instalar o certificado da Kaspersky Lab:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione o componente **Rede**.
3. Na janela que é aberta, marque a caixa **Verificar conexões criptografadas**. Quando você ativar essa configuração pela primeira vez, o Assistente para Instalação de Certificados será executado automaticamente.
4. Se o assistente não for iniciado, clique no botão **Instalar certificado**. Será iniciado um assistente com instruções a serem seguidas para a instalação bem-sucedida do certificado da Kaspersky Lab.

NESTA SEÇÃO:

Verificando conexões criptografadas no Mozilla Firefox 115

Verificando conexões criptografadas no Opera 115

VERIFICANDO CONEXÕES CRIPTOGRAFADAS NO MOZILLA FIREFOX

O navegador Mozilla Firefox não usa o armazenamento de certificados do Microsoft Windows. Para verificar conexões SSL ao usar o Firefox, você deve instalar manualmente o certificado da Kaspersky Lab.

Você poderá usar o Assistente para Instalação de Certificados caso o navegador não seja executado.

Para instalar o certificado da Kaspersky Lab manualmente:

1. No menu do navegador, selecione o item **Ferramentas** →**Configurações**.
2. Na janela que é aberta, selecione a seção **Additional**.
3. Na seção **Certificados**, selecione a guia **Segurança** e clique no botão **Exibir Certificados**.
4. Na janela que é aberta, selecione a guia **Autoridades** e clique no botão **Restaurar**.
5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que é aberta, marque as caixas para selecionar as ações que devem ser verificadas com o certificado instalado. Para exibir as informações do certificado, clique no botão **Exibir**.

Para instalar o certificado para o Mozilla Firefox versão 3.x:

1. No menu do navegador, selecione o item **Ferramentas** →**Configurações**.
2. Na janela que é aberta, selecione a seção **Additional**.
3. Na guia **Criptografia**, clique no botão **Exibir Certificados**.
4. Na janela que é aberta, selecione a guia **Autoridades** e clique no botão **Importar**.
5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que é aberta, marque as caixas para selecionar as ações que devem ser verificadas com o certificado instalado. Para exibir as informações do certificado, clique no botão **Exibir**.

Se o computador for executado com o Microsoft Windows Vista ou o Microsoft Windows 7, o caminho do arquivo do certificado da Kaspersky Lab será o seguinte: *%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

VERIFICANDO CONEXÕES CRIPTOGRAFADAS NO OPERA

O navegador Opera não usa o armazenamento de certificados do Microsoft Windows. Para verificar conexões SSL ao usar o Opera, você deve instalar o certificado da Kaspersky Lab manualmente.

Para instalar o certificado da Kaspersky Lab:

1. No menu do navegador, selecione o item **Ferramentas** →**Configurações**.
2. Na janela que é aberta, selecione a seção **Additional**.
3. À esquerda da janela, selecione a guia **Security** e clique no botão **Manage Certificates**.
4. Na janela que é aberta, selecione a guia **Vendors** e clique no botão **Import**.
5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que é aberta, clique no botão **Install**. O certificado da Kaspersky Lab é instalado. Para exibir as informações do certificado e selecionar as ações para as quais ele será usado, selecione o certificado na lista e clique no botão **View**.

Para instalar o certificado da Kaspersky Lab para o Opera versão 9.x:

1. No menu do navegador, selecione o item **Ferramentas** →**Configurações**.
2. Na janela que é aberta, selecione a seção **Additional**.
3. À esquerda da janela, selecione a guia **Security** e clique no botão **Manage Certificates**.
4. Na janela que é aberta, selecione a guia **Autoridades** e clique no botão **Importar**.
5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Na janela que é aberta, clique no botão **Install**. O certificado da Kaspersky Lab é instalado.

Se o computador for executado com o Microsoft Windows Vista ou o Microsoft Windows 7, o caminho do arquivo do certificado da Kaspersky Lab será o seguinte: *%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

CONFIGURANDO O SERVIDOR PROXY

Se a conexão do computador com a Internet for estabelecida através de um servidor proxy, talvez seja necessário editar suas configurações de conexão. O Kaspersky Anti-Virus usa essas configurações para determinados componentes de proteção e para atualizar os bancos de dados e módulos do aplicativo.

Se a sua rede incluir um servidor proxy que usa uma porta diferente do padrão, adicione o número da porta à lista de portas monitoradas (consulte a seção "Criando uma lista de portas monitoradas" na página 117).

Para configurar o servidor proxy:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione o componente **Rede**.
3. Na seção **Servidor proxy**, clique no botão **Configurações do servidor proxy**.
4. Na janela **Configurações do servidor proxy** que é aberta, modifique as configurações do servidor proxy.

CRIANDO UMA LISTA DE PORTAS MONITORADAS

Os componentes de proteção, como o Antivírus de Email, Antivírus da Web (na página 101), e Antivírus de IM, monitoram os fluxos de dados transferidos por protocolos específicos e que passam por determinadas portas TCP abertas no computador. Por exemplo, o Antivírus de Email verifica as informações transferidas por SMTP, enquanto o Antivírus da verifica as informações transferidas por HTTP, HTTPS e FTP.

Você pode ativar o monitoramento completo ou apenas das portas de rede selecionadas. Se você configurar o produto para monitorar as portas selecionadas, poderá especificar a lista de aplicativos para os quais todas as portas serão monitoradas. É recomendável expandir a lista incluindo os aplicativos que recebem ou transferem dados por FTP.

Para adicionar uma porta à lista de portas monitoradas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione o componente **Rede**.
3. Na seção **Portas monitoradas**, selecione **Monitorar somente as portas selecionadas** e clique no botão **Selecionar**.

   A janela **Portas de rede** é aberta.
4. Clique no link **Adicionar** sob a lista de portas na parte superior da janela para abrir a janela **Porta de rede** e insira o número e a descrição da porta.

Para excluir uma porta da lista de portas monitoradas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione o componente **Rede**.
3. Na seção **Portas monitoradas**, selecione **Monitorar somente as portas selecionadas** e clique no botão **Selecionar**.

   A janela **Portas de rede** é aberta.
4. Na lista de portas na parte superior da janela, desmarque a caixa ao lado da descrição da porta que deve ser excluída.

Para criar a lista de aplicativos para os quais você deseja monitorar todas as portas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione o componente **Rede**.
3. Na seção **Portas monitoradas**, selecione **Monitorar somente as portas selecionadas** e clique no botão **Selecionar**.

   A janela **Portas de rede** é aberta.
4. Marque a caixa **Monitorar todas as portas para os aplicativos especificados** e, na lista de aplicativos abaixo, marque as caixas correspondentes aos nomes dos aplicativos para os quais todas as portas devem ser monitoradas.
5. Se um aplicativo não estiver incluído na lista, adicione-o da seguinte maneira:

   a. Para selecionar um método para adicionar um aplicativo à lista, abra o menu clicando no link **Adicionar** abaixo da lista de aplicativos e selecione um item no menu:

      - Selecione **Procurar** para especificar o local do arquivo executável. Depois de ter selecionado o arquivo executável, a janela **Aplicativo** será aberta.

- Selecione **Aplicativos** para selecionar um aplicativo na lista de aplicativos ativos no momento. Depois de ter selecionado um aplicativo na lista, a janela **Aplicativo** será aberta.

b. Na janela **Aplicativo**, insira a descrição do aplicativo selecionado.

ZONA CONFIÁVEL

A *zona confiável* consiste em uma lista criada pelo usuário de objetos que não serão controlados pelo aplicativo. Em outras palavras, é um conjunto de exclusões do escopo de proteção do Kaspersky Anti-Virus.

A zona confiável é criada com base na lista de aplicativos confiáveis (consulte a seção "Criando uma lista de aplicativos confiáveis" na página 119) e em regras de exclusão (consulte a seção "Criando as regras de exclusão" na página 119) referentes às características dos objetos processados e dos aplicativos instalados no computador. Talvez seja necessário incluir objetos na zona confiável se, por exemplo, o Kaspersky Anti-Virus bloquear o acesso a um objeto ou aplicativo embora você tenha certeza de que ele é absolutamente inofensivo.

Por exemplo, se você acha que os objetos usados pelo Bloco de Notas do Microsoft Windows são inofensivos e não precisam ser verificados, ou seja, se você confia nesse aplicativo, adicione o Bloco de Notas à lista de aplicativos confiáveis para excluir a verificação dos objetos usados por esse processo.

Algumas ações classificadas como perigosas podem ser consideradas seguras por vários aplicativos. Assim, os aplicativos que alternam automaticamente o layout do teclado, como o Punto Switcher, normalmente interceptam o texto digitado no teclado. Para considerar as especificidades desses aplicativos e desativar o monitoramento de suas atividades, é recomendável adicioná-los à lista de aplicativos confiáveis.

Quando um aplicativo é adicionado à lista de aplicativos confiáveis, suas atividades de rede e com arquivos (inclusive as suspeitas) não são mais controladas. O mesmo ocorre com suas tentativas de acesso ao Registro do sistema. Ao mesmo tempo, o arquivo executável e o processo do aplicativo confiável são verificados quanto à presença de vírus, como anteriormente. Para excluir completamente o aplicativo da verificação, use as regras de exclusão.

A exclusão de aplicativos confiáveis da verificação permite evitar problemas de compatibilidade do aplicativo com outros programas (por exemplo, a verificação duplicada do tráfego de rede de um computador de terceiros pelo Kaspersky Anti-Virus e por outro aplicativo antivírus), além de melhorar o desempenho do computador, que é crítico ao usar aplicativos de servidor.

Por sua vez, as regras de exclusão da zona confiável garantem a opção de trabalhar com aplicativos legais que podem ser usadas por invasores para danificar o computador ou os dados do usuário. Esses aplicativos não têm recursos maliciosos, mas podem ser usados como componentes auxiliares de um programa malicioso. Esta categoria inclui aplicativos de administração remota, programas de IRC, servidores FTP, diversos utilitários para interromper ou ocultar processos, programas de registro do teclado, programas de quebra de senhas, discadores e outros. Esses aplicativos podem ser bloqueados pelo Kaspersky Anti-Virus. Para evitar o bloqueio, você pode configurar regras de exclusão.

Regra de exclusão – é um conjunto de condições que determinam que um objeto não deve ser verificado pelo Kaspersky Anti-Virus. Em qualquer outro caso, o objeto é verificado por todos os componentes de proteção de acordo com suas respectivas configurações de proteção.

As regras de exclusão da zona confiável podem ser usadas por vários componentes do aplicativo, como o Antivírus de Arquivos, o Antivírus de Email, o Antivírus da Web (consulte a seção "Antivírus da Web" na página 101) ou ao executar tarefas de verificação de vírus.

NESTA SEÇÃO:

Criando uma lista de aplicativos confiáveis 119

Criando as regras de exclusão 119

CRIANDO UMA LISTA DE APLICATIVOS CONFIÁVEIS

Por padrão, o Kaspersky Anti-Virus verifica os objetos abertos, executados ou salvos pelos processos de todos os programas e monitora a atividade de todos os aplicativos e do tráfego de rede criado por eles. Quando você adiciona um aplicativo à lista de confiáveis, o Kaspersky Anti-Virus o exclui da verificação.

Para adicionar um aplicativo à lista confiável:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Ameaças e Exclusões**.
3. Na seção **Exclusões**, clique no botão **Configurações**.
4. Na janela que é aberta, na guia **Aplicativos confiáveis**, abra o menu de seleção de aplicativos clicando no botão **Adicionar**.
5. No menu que é aberto, selecione um aplicativo da lista **Aplicativos** ou selecione **Procurar** para especificar o caminho dos arquivos executáveis do aplicativo desejado.
6. Na janela **Exclusões do aplicativo** que é aberta, marque as caixas correspondentes aos tipos de atividades do aplicativo que devem ser excluídos da verificação.

Você pode alterar um aplicativo confiável ou excluí-lo da lista usando os botões correspondentes na parte superior da janela. Para remover um aplicativo da lista sem excluí-lo, desmarque a caixa ao lado de seu nome.

CRIANDO AS REGRAS DE EXCLUSÃO

Se você usar aplicativos reconhecidos pelo Kaspersky Anti-Virus como legais, mas que podem ser usados por invasores para danificar o computador ou os dados do usuário, é recomendável configurar regras de exclusão para eles.

Para criar uma regra de exclusão:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Ameaças e Exclusões**.
3. Na seção **Exclusões**, clique no botão **Configurações**.
4. Na janela que é aberta, na guia **Regras de exclusão**, clique no botão **Adicionar**.
5. Na janela **Regra de exclusão** que é aberta, edite as configurações da regra de exclusão.

DESEMPENHO E COMPATIBILIDADE COM OUTROS APLICATIVOS

O desempenho do Kaspersky Anti-Virus depende do intervalo de ameaças que podem ser detectadas, do consumo de energia e da intensidade de uso de recursos.

O Kaspersky Anti-Virus permite configurar de forma flexível o escopo de proteção e selecionar vários tipos de ameaças (consulte a seção "Selecionando as categorias de ameaças detectáveis" na página 120) que devem ser detectadas pelo aplicativo.

O consumo de energia é muito importante para computadores portáteis. Muitas vezes, a verificação de computadores quanto à presença de vírus e a atualização dos bancos de dados do Kaspersky Anti-Virus exigem recursos significativos. O modo para laptops do Kaspersky Anti-Virus (veja a página 122) permite adiar automaticamente tarefas de atualização e verificação programadas ao trabalhar com a bateria, economizando sua carga, enquanto o modo de

Verificação Ociosa (consulte a seção "Executando tarefas em background" na página 121) permite executar tarefas que utilizam muitos recursos quando o computador não está sendo usado.

A utilização de recursos do computador pelo Kaspersky Anti-Virus pode afetar o desempenho de outros aplicativos. Para resolver problemas de operações simultâneas com grande exigências dos subsistemas de disco e da CPU, o Kaspersky Anti-Virus pode pausar as tarefas de verificação e conceder recursos a outros aplicativos (veja a página 121) em execução no computador.

No modo Perfil de jogo, o aplicativo desativa automaticamente a exibição de notificações sobre atividades do Kaspersky Anti-Virus quando há outros aplicativos em execução no modo de tela inteira.

No caso de uma infecção ativa no sistema, o procedimento de desinfecção avançada exige o reinício do computador, o que também pode afetar o desempenho de outros aplicativos. Se necessário, é possível desativar a tecnologia de desinfecção avançada (veja a página 120) para evitar o reinício indesejado do computador.

NESTA SEÇÃO:

Selecionando as categorias de ameaças detectáveis 120

Tecnologia de desinfecção avançada 120

Distribuindo os recursos do computador durante a verificação de vírus 121

Executando tarefas em background 121

Configurações do aplicativo no modo de tela inteira. Perfil de Jogo 122

Economia de bateria 122

SELECIONANDO AS CATEGORIAS DE AMEAÇAS DETECTÁVEIS

As ameaças detectadas pelo Kaspersky Anti-Virus estão divididas em categorias de acordo com vários atributos. O aplicativo sempre detecta vírus, cavalos de Troia e ferramentas de utilitários maliciosos. Esses programas podem causar danos significativos ao computador. Para garantir a proteção mais confiável do computador, você pode estender a lista de ameaças detectadas ativando o controle de ações executadas por aplicativos legais que podem ser usadas por um invasor para danificar o computador e os dados do usuário.

- *Para selecionar as categorias de ameaças que podem ser detectadas:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Ameaças e Exclusões**.
  3. À direita da janela, clique no botão **Configurações** abaixo da lista **A detecção dos seguintes tipos de ameaças está ativada**.
  4. Na janela **Ameaças** que é aberta, marque as caixas correspondentes às categorias de ameaças que devem ser detectadas.

TECNOLOGIA DE DESINFECÇÃO AVANÇADA

Os programas maliciosos atuais conseguem invadir os níveis mais baixos de um sistema operacional, o que torna praticamente impossível excluí-los. Se for detectada alguma atividade maliciosa no sistema, o Kaspersky Anti-Virus poderá realizar um procedimento especial de desinfecção avançada que permitirá eliminar a ameaça e excluí-la do computador.

Após esse procedimento, será necessário reiniciar o computador. Depois de reiniciar o computador, é recomendável executar a verificação completa de vírus (consulte a seção "Como executar a verificação completa do computador quanto à presença de vírus" na página 60).

Para que o Kaspersky Anti-Virus inicie o procedimento de desinfecção avançada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Compatibilidade**.
3. Marque a caixa **Ativar Tecnologia de desinfecção avançada**.

DISTRIBUINDO OS RECURSOS DO COMPUTADOR DURANTE A VERIFICAÇÃO DE VÍRUS

As tarefas de verificação de vírus podem ser adiadas a fim de limitar a carga da CPU e dos subsistemas de armazenamento em disco.

A execução de tarefas de verificação aumenta a carga da CPU e dos subsistemas de disco, tornando os outros aplicativos mais lentos. Por padrão, se isso acontecer, o Kaspersky Anti-Virus pausará as tarefas de verificação de vírus e liberará os recursos do sistema para os aplicativos do usuário.

Entretanto, vários aplicativos serão iniciados imediatamente quando os recursos da CPU estiverem disponíveis, sendo executados em background. Para que a verificação não dependa do desempenho desses aplicativos, os recursos do sistema não devem ser disponibilizados para eles.

Esta configuração pode ser definida individualmente para cada tarefa de verificação. Nesse caso, a configuração de uma tarefa específica terá prioridade maior.

Para adiar a execução das tarefas de verificação pelo Kaspersky Anti-Virus, caso isso torne outros aplicativos mais lentos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Compatibilidade**.
3. Marque a caixa **Conceder recursos a outros aplicativos**.

EXECUTANDO TAREFAS EM BACKGROUND

Para otimizar a carga sobre os recursos do computador, você pode ativar a verificação normal de rootkits em background e a execução de tarefas que utilizam muitos recursos quando o computador estiver ocioso.

A verificação normal de rootkits é executada enquanto você trabalha no computador. A verificação leva no máximo cinco minutos e envolve uma parcela mínima dos recursos do computador.

Quando o computador está ocioso, as seguintes tarefas podem ser executadas:

- atualização automática dos bancos de dados de antivírus e módulos do programa;
- verificação da memória do sistema, dos objetos de inicialização e da partição do sistema.

As tarefas de Verificação Ociosa serão executadas se o computador tiver sido bloqueado pelo usuário ou se a proteção de tela for exibida na tela por pelo menos cinco minutos.

Se o computador estiver trabalhando com a bateria, nenhuma tarefa será executada, mesmo que o computador esteja ocioso.

O primeiro estágio da Verificação Ociosa consiste em verificar se os bancos de dados e módulos do aplicativo estão atualizados. Se for necessária uma atualização após a verificação, a tarefa de atualização automática será iniciada. No segundo estágio, o aplicativo verifica a data e o status da última execução da Verificação Ociosa. Se a Verificação Ociosa ainda não tiver sido executada, tiver sido executada mais de sete dias atrás ou tiver sido interrompida, o

aplicativo executará a tarefa de verificação da memória do sistema, dos objetos de inicialização e do Registro do sistema.

A Verificação Ociosa é executada no nível profundo de análise heurística, o que aumenta a probabilidade de detecção de ameças.

Quando o usuário voltar ao trabalho, a tarefa de Verificação Ociosa será interrompida automaticamente. O aplicativo lembra o estágio em que a tarefa foi interrompida para reiniciar a verificação a partir desse ponto no futuro.

Se a execução das tarefas de Verificação Ociosa tiver sido interrompida durante o download do pacote de atualização, a atualização será iniciada do começo da próxima vez.

- *Para ativar a verificação normal de rootkits em background:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a subseção **Configurações Gerais**.
  3. À direita da janela, marque a caixa **Executar verificação normal de rootkits**.

- *Para ativar o modo de Verificação Ociosa:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a subseção **Configurações Gerais**.
  3. À direita da janela, marque a caixa **Executar verificação ociosa**.

CONFIGURAÇÕES DO APLICATIVO NO MODO DE TELA INTEIRA. PERFIL DE JOGO

Alguns aplicativos (especialmente os videogames) que são executados no modo de tela inteira são pouco compatíveis com alguns recursos do Kaspersky Anti-Virus: por exemplo, as notificações pop-up são totalmente indesejáveis nesse modo. Frequentemente esses aplicativos exigem recursos significativos do sistema, de forma que a execução de algumas tarefas do Kaspersky Anti-Virus pode reduzir seu desempenho.

Para que não seja necessário desativar manualmente as notificações e pausar as tarefas sempre que você executar aplicativos em tela inteira, o Kaspersky Anti-Virus oferece a opção de editar temporariamente as configurações, usando o perfil de jogo. Quando o Perfil de Jogo está ativo, ao alternar para o modo de tela inteira as configurações de todos os componentes do produto são alteradas automaticamente para assegurar o funcionamento ideal do sistema. Ao sair do modo de tela inteira, as configurações do produto retornam aos valores iniciais usados antes de entrar nesse modo.

- *Para ativar o perfil de jogo:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Perfil de Jogo**.
  3. Marque a caixa **Usar Perfil de Jogo** e, na seção **Opções do perfil** abaixo, especifique as configurações de perfil de jogo desejadas.

ECONOMIA DE BATERIA

Para economizar energia em um computador portátil, as tarefas de verificação de vírus e atualização programada podem ser adiadas. Se necessário, você pode atualizar o Kaspersky Anti-Virus ou iniciar uma verificação de vírus manualmente.

Para ativar o modo de economia de energia e prorrogar a vida útil da bateria:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Economia de Bateria**.
3. À direita da janela, marque a caixa **Desativar verificações programadas ao trabalhar com a bateria**.

AUTODEFESA DO KASPERSKY ANTI-VIRUS

Como o Kaspersky Anti-Virus assegura a proteção do computador contra malware, programas maliciosos que invadem o computador tentam bloquear o Kaspersky Anti-Virus ou até mesmo excluir o aplicativo do computador.

O desempenho estável do sistema de segurança do computador é garantido através dos recursos de autodefesa e proteção contra acesso remoto implementados no Kaspersky Anti-Virus.

A autodefesa do Kaspersky Anti-Virus evita a modificação e exclusão de seus próprios arquivos do disco rígido, de processos na memória e de entradas no Registro do sistema. A proteção contra acesso remoto permite bloquear todas as tentativas de controlar remotamente serviços de aplicativos.

Nos computadores que executam sistemas operacionais de 64 bits e o Microsoft Windows Vista, a Autodefesa do Kaspersky Anti-Virus estará disponível apenas para evitar que os arquivos do próprio aplicativo em unidades locais e o Registro do sistema sejam modificados ou excluídos.

NESTA SEÇÃO:

Ativando e desativando a autodefesa 123

Proteção contra o controle externo 123

ATIVANDO E DESATIVANDO A AUTODEFESA

Por padrão, a autodefesa do Kaspersky Anti-Virus está ativada. Se necessário, você pode desativar a autodefesa.

Para desativar a Autodefesa do Kaspersky Anti-Virus:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Autodefesa**.
3. À direita da janela, desmarque a caixa **Ativar Autodefesa**.

PROTEÇÃO CONTRA O CONTROLE EXTERNO

Por padrão, a proteção contra controle externo está ativada. Se necessário, você pode desativar a proteção.

São frequentes as situações em que programas de administração remota (como o RemoteAdmin) são necessários ao usar a proteção contra acesso remoto. Para assegurar o desempenho normal desses aplicativos, adicione-os à lista de aplicativos confiáveis (consulte a seção "Criando uma lista de aplicativos confiáveis" na página 119) e ative a configuração **Não monitorar a atividade de aplicativos** correspondente.

Para desativar a proteção contra o controle externo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Autodefesa**.
3. Na seção **Controle externo**, desmarque a caixa **Desativar controle de serviços externos**.

QUARENTENA E BACKUP

A *Quarentena* é um repositório especial que armazena os objetos possivelmente infectados por vírus. *Objetos possivelmente infectados* são objetos suspeitos de estarem infectados por vírus ou modificações deles.

Um objeto possivelmente infectado pode ser detectado e colocado na Quarentena pelo Antivírus de Arquivos, pelo Antivírus de Email, pela Defesa Proativa ou durante uma verificação de vírus.

Os objetos são colocados na Quarentena nos seguintes casos:

- O código do objeto lembra uma ameaça conhecida, mas parcialmente modificado, ou tem uma estrutura semelhante à de malware, mas não está registrado no banco de dados. Nesse caso, os objetos são movidos para a Quarentena depois da análise heurística executada pelo Antivírus de Arquivos, pelo Antivírus de Email ou durante a verificação antivírus. A análise heurística raramente gera falsos positivos.
- A sequência de operações executadas por um objeto parece suspeita. Nesse caso, os objetos são movidos para a Quarentena após a análise de seu comportamento pelo componente Defesa Proativa.

Ao colocar um objeto na Quarentena, ele é movido e não copiado; o objeto é excluído do disco ou do email e salvo na pasta Quarentena. Os arquivos na Quarentena são salvos em um formato especial e não são perigosos.

O *armazenamento de Backup* se destina ao armazenamento de cópias de backup de objetos infectados que não puderam ser desinfetados imediatamente após a detecção.

É possível que, após a próxima atualização dos bancos de dados, o Kaspersky Anti-Virus possa identificar a ameaça com segurança e neutralizá-la. Por isso, o aplicativo verifica os objetos da Quarentena após cada atualização (veja a página 89).

NESTA SEÇÃO:

Armazenando objetos da Quarentena e do Backup 124

Trabalhando com objetos da Quarentena 125

ARMAZENANDO OBJETOS DA QUARENTENA E DO BACKUP

O período máximo padrão de armazenamento de objetos é de 30 dias. Depois disso, os objetos serão excluídos. Você pode cancelar a restrição de tempo ou alterar a duração máxima do armazenamento de objetos.

Além disso, é possível especificar o tamanho máximo da Quarentena e do Backup. Quando ele for atingido, o conteúdo da Quarentena e do Backup será substituído por novos objetos. Por padrão, a restrição do tamanho máximo está desativada.

Para modificar o tempo máximo de armazenamento de objetos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.

3. À direita da janela, na seção **Armazenando objetos da Quarentena e do Backup**, marque a caixa **Armazenar objetos por no máximo** e especifique o período máximo de armazenamento de objetos em quarentena.

Para configurar o tamanho máximo da Quarentena e do Backup:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
3. À direita da janela, na seção **Armazenando objetos da Quarentena e do Backup**, marque a caixa **Tamanho máximo** e especifique o tamanho máximo da Quarentena e do Backup.

TRABALHANDO COM OBJETOS DA QUARENTENA

A Quarentena do Kaspersky Anti-Virus permite executar as seguintes operações:

- colocar na Quarentena os arquivos que suspeita estarem infectados;
- verificar e desinfetar todos os objetos possivelmente infectados da Quarentena usando os bancos de dados atuais do Kaspersky Anti-Virus;
- restaurar os arquivos de uma pasta especificada para as pastas de origem das quais eles foram movidos para a Quarentena (por padrão);
- excluir qualquer objeto ou grupo de objetos da Quarentena;
- enviar os objetos da Quarentena à Kaspersky Lab para análise.

Você pode mover um objeto para a Quarentena usando um dos métodos a seguir:

- usando o link **Mover para a Quarentena** na janela **Estado de proteção**;
- usando o menu de contexto do objeto.

Para mover um objeto para a Quarentena na janela Estado de proteção:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela principal para abrir a janela **Estado de proteção** na guia **Ameaças detectadas**.
3. Clique no botão **Mover para a Quarentena**.
4. Na janela que é aberta, selecione o objeto que você deseja mover para a Quarentena.

Para mover um objeto para a Quarentena usando o menu de contexto:

1. Abra o Microsoft Windows Explorer e vá para a pasta que contém o objeto que você deseja mover para a Quarentena.
2. Clique com o botão direito do mouse no menu de contexto do objeto e selecione **Mover para a Quarentena**.

Para verificar um objeto da Quarentena:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela e abra a janela da Quarentena.
3. Na janela que é aberta, na guia **Ameaças detectadas**, selecione o objeto que deve ser verificado.

4. Clique com o botão direito do mouse nos arquivos desejados para abrir o menu de contexto e selecione **Verificar**.

Para desinfetar todos os objetos da Quarentena:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela e abra a janela da Quarentena.
3. Na janela que é aberta, na guia **Ameaças detectadas**, clique no botão **Desinfetar tudo**.

Para restaurar um objeto da Quarentena:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela e abra a janela da Quarentena.
3. Na janela que é aberta, na guia **Ameaças detectadas**, selecione o objeto que deve ser restaurado.
4. Clique com o botão direito do mouse nos arquivos desejados para abrir o menu de contexto e selecione **Restaurar**.

Para remover objetos da Quarentena:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela e abra a janela da Quarentena.
3. Na janela que é aberta, na guia **Ameaças detectadas**, selecione o objeto que deve ser removido.
4. Clique com o botão direito do mouse no objeto desejado para abrir o menu de contexto e selecione **Excluir da lista**.

Para enviar um objeto da Quarentena à Kaspersky Lab para análise:

1. Abra a janela principal do aplicativo.
2. Clique no link **Quarentena** na parte superior da janela e abra a janela da Quarentena.
3. Na janela que é aberta, na guia **Ameaças detectadas**, selecione o objeto que deve ser enviado para análise.
4. Clique com o botão direito do mouse no objeto desejado para abrir o menu de contexto e selecione **Enviar**.

FERRAMENTAS ADICIONAIS PARA PROTEGER MELHOR SEU COMPUTADOR

Os seguintes assistentes e ferramentas fornecidos com o Kaspersky Anti-Virus são usados para resolver problemas específicos referentes à segurança do computador:

- O Assistente para Criação do Disco de Recuperação foi criado para criar o Disco de Recuperação, que permite restaurar a funcionalidade do sistema após um ataque de vírus através da inicialização do computador a partir de uma mídia removível. O Disco de Recuperação deve ser usado quando o nível de infecção torna impossível desinfetar o computador usando aplicativos antivírus ou utilitários de remoção de malware.
- O Assistente de Limpeza de Dados Particulares foi criado para pesquisar e eliminar rastros das atividades de um usuário no sistema e as configurações do sistema operacional que permitem coletar informações sobre as atividades do usuário.

- O Assistente de Restauração do Sistema foi criado para eliminar danos e rastros de objetos de malware do sistema.

- Assistente de Configuração do Navegador foi criado para analisar e ajustar as configurações do Microsoft Internet Explorer a fim de eliminar as possíveis vulnerabilidades.

- A Verificação de Vulnerabilidades foi criada para diagnosticar vulnerabilidades no sistema operacional e nos aplicativos instalados a fim de detectar violações de segurança que possam ser exploradas por invasores.

Todos os problemas encontrados pelos Assistentes (exceto o Assistente para Criação do Disco de Recuperação) são apresentados em grupos, de acordo com o tipo de perigo que representam para o sistema operacional. A Kaspersky Lab oferece um conjunto de ações para cada grupo de problemas que ajudam a eliminar vulnerabilidades e pontos frágeis nas configurações do sistema. Existem três grupos de problemas e três grupos de ações a serem executadas com eles, quando detectados:

- *Ações altamente recomendadas* ajudarão a eliminar problemas que representam uma ameaça de segurança grave. É recomendável executar todas as ações desse grupo oportunamente a fim de eliminar a ameaça.

- *Ações recomendadas* eliminam problemas que representam uma possível ameaça. Também é recomendável executar todas as ações desse grupo para ter o nível ideal de proteção.

- *Ações adicionais* ajudam a reparar danos ao sistema que não representam uma ameaça atual, mas que podem ameaçar a segurança do computador no futuro. A execução dessas ações garante a proteção abrangente do computador. Contudo, em alguns casos, elas podem levar à exclusão das configurações do usuário (como cookies).

NESTA SEÇÃO:

Limpeza de Dados Particulares 127

Configuração do Navegador 128

Revertendo as alterações executadas pelos assistentes..... 130

LIMPEZA DE DADOS PARTICULARES

Ao trabalhar com o computador, as ações do usuário são registradas no sistema. Os dados gravados incluem as consultas de pesquisa inseridas por usuários e os sites visitados, os programas executados, os arquivos abertos e salvos, o log de eventos do Microsoft Windows, arquivos temporários, etc.

Todas essas fontes de informações sobre as atividades do usuário podem conter dados confidenciais (incluindo senhas) e podem estar disponíveis para serem analisadas por invasores. Frequentemente, o usuário não tem conhecimento suficiente para evitar que informações dessas fontes sejam roubadas.

O Kaspersky Anti-Virus inclui o Assistente de limpeza de dados particulares. O Assistente procura rastros de atividades do usuário no sistema, além de configurações do sistema operacional que contribuem para o armazenamento de informações sobre as atividades do usuário.

Lembre-se de que os dados relacionados à atividade do usuário no sistema são acumulados continuamente. A execução de qualquer arquivo ou a abertura de qualquer documento são registradas. O log do sistema Microsoft Windows registra vários eventos que ocorrem no sistema. Por isso, a execução repetida do Assistente de Limpeza de Dados Particulares pode detectar rastros de atividades que não foram apagados pela execução anterior do Assistente. Alguns arquivos, como o arquivo de log do Microsoft Windows, podem estar em uso pelo sistema enquanto o Assistente tenta excluí-los. Para excluir esses arquivos, o Assistente irá sugerir que você reinicie o sistema. Entretanto, ao reiniciar, esses arquivos podem ser recriados e detectados novamente como rastros de atividades.

O Assistente consiste em uma série de telas (etapas) nas quais você navega usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Para iniciar o Assistente de Limpeza de Dados Particulares:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** à esquerda da janela.
2. À direita da janela, clique no botão **Limpeza de Dados Particulares**.

As etapas detalhadas do Assistente.

Step 1. Iniciando o Assistente

Confirme se a opção **Executar diagnóstico de rastros de atividades do usuário** está selecionada e clique no botão **Avançar** para iniciar o Assistente.

Step 2. Pesquisa de sinais de atividade

Este assistente pesquisa rastros de atividades de malware no computador. A verificação pode levar algum tempo. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 3. Selecionando as ações de Limpeza de Dados Particulares

Ao concluir a pesquisa, o Assistente exibe os rastros de atividades detectados e as ações sugeridas para eliminá-los. O relatório de atividades do Assistente é exibido no formato de lista (consulte a seção "Ferramentas adicionais para proteger melhor seu computador" na página 126).

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

É altamente recomendável não desmarcar as caixas selecionadas por padrão, pois isso pode deixar o computador vulnerável a ameaças.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Step 4. Limpeza de Dados Particulares

O Assistente executará as ações selecionadas na etapa anterior. A eliminação dos rastros de atividades pode levar algum tempo. Para limpar determinados rastros de atividades, pode ser necessário reiniciar o computador; você será notificado pelo Assistente.

Quando a limpeza for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 5. Conclusão do Assistente

Se desejar limpar todos os rastros de atividades do usuário automaticamente sempre que o Kaspersky Anti-Virus concluir o trabalho, na última etapa do Assistente, marque a caixa **Limpar rastros de atividades sempre ao sair do Kaspersky Anti-Virus**. Se desejar remover os rastros de atividades manualmente usando o Assistente, não marque essa caixa.

Clique no botão **Concluir** para fechar o assistente.

CONFIGURAÇÃO DO NAVEGADOR

Em determinadas situações, o navegador Microsoft Internet Explorer exige uma análise e configuração especial, pois alguns valores selecionados pelo usuário ou definidos por padrão podem causas problemas de segurança.

Seguem alguns exemplos dos objetos e parâmetros usados no navegador e suas associações a possíveis ameaças de segurança:

- **Cache do Microsoft Internet Explorer**. O cache armazena dados baixados da Internet, permitindo que eles não sejam baixados da próxima vez. Assim, é possível reduzir o tempo de carregamento de páginas da Web e economizar tráfego da Internet. Além disso, o cache contém dados confidenciais, dos quais é possível obter também um histórico dos sites visitados pelo usuário. Alguns objetos de malware examinam o cache ao verificar o disco e os invasores podem obter, por exemplo, os endereços de email do usuário. É recomendável limpar o cache sempre que você fechar o navegador para melhorar a proteção.

- **Exibição de extensões de tipos de arquivos conhecidos**. Para editar os nomes de arquivos de forma conveniente, você pode desativar a exibição de suas extensões. Contudo, às vezes é útil ver a extensão do arquivo. Os nomes de arquivo de vários objetos maliciosos contêm combinações de símbolos que simulam uma extensão de arquivo adicional antes da extensão real (por exemplo, exemplo.txt.com). Se a extensão do arquivo real não for exibida, os usuários poderão ver apenas a parte do nome de arquivo com a extensão simulada e, assim, poderão identificar um objeto malicioso como um arquivo inofensivo. Para melhorar a proteção, é recomendável ativar a exibição de arquivos de formatos conhecidos.

- **Lista de sites confiáveis**. Para que alguns sites sejam executados corretamente, você deve adicioná-los à lista de sites confiáveis. Ao mesmo tempo, objetos maliciosos podem adicionar a essa lista links para sites criados por invasores.

Algumas configurações podem resultar em problemas com a exibição de determinados sites (por exemplo, se eles usarem controles ActiveX). Esse problema pode ser resolvido adicionando esses sites à zona confiável.

A análise e a configuração do navegador são executadas no Assistente de Configuração do Navegador. O assistente verifica se as últimas atualizações do navegador estão instaladas e confirma se as configurações atuais do navegador não tornam o sistema vulnerável a explorações maliciosas. Ao concluir o Assistente, será gerado um relatório que pode ser enviado à Kaspersky Lab para análise.

O Assistente consiste em uma série de telas (etapas) nas quais você navega usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Feche todas as janelas do Microsoft Internet Explorer antes de iniciar o diagnóstico.

Para iniciar o Assistente de Configuração do Navegador:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** à esquerda da janela.
2. Clique no botão **Configuração do Navegador** à direita da janela.

As etapas detalhadas do Assistente.

Step 1. Iniciando o Assistente

Confirme se a opção **Executar o diagnóstico do Microsoft Internet Explorer** está selecionada e clique no botão **Avançar** para iniciar o Assistente.

Step 2. Análise de configurações do Microsoft Internet Explorer

O assistente analisa as configurações do Microsoft Internet Explorer. A pesquisa de problemas nas configurações do navegador pode levar algum tempo. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 3. Selecionando as ações para configurar o navegador

Os problemas detectados na etapa anterior são agrupados de acordo com o nível de perigo para o sistema que representam (consulte a seção "Ferramentas adicionais para proteger melhor seu computador" na página 126).

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

É altamente recomendável não desmarcar as caixas selecionadas por padrão, pois isso pode deixar o computador vulnerável a ameaças.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Step 4. Configuração do Navegador

O Assistente executará as ações selecionadas na etapa anterior. A configuração do navegador pode levar algum tempo. Quando a configuração for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 5. Conclusão do Assistente

Clique no botão **Concluir** para fechar o assistente.

REVERTENDO AS ALTERAÇÕES EXECUTADAS PELOS ASSISTENTES

É possível reverter (cancelar) algumas alterações feitas ao iniciar o Assistente de Limpeza de Dados Particulares (consulte a seção "Eliminando rastros de atividade" na página 127), o Assistente de Restauração do Sistema (consulte a seção "O que fazer se você suspeitar que o computador está infectado" na página 64) e o Assistente de Configuração do Navegador (consulte a seção "Configuração do navegador" na página 128).

Para reverter as alterações, execute o assistente correspondente da seguinte maneira:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** à esquerda da janela.
2. À direita da janela, clique em um dos seguintes botões:
   - **Limpeza de Dados Particulares** – para iniciar o Assistente de Limpeza de Dados Particulares;
   - **Restauração do Sistema** – para iniciar o Assistente de Restauração do Sistema;
   - **Configuração do Navegador** – para iniciar o Assistente de Configuração do Navegador.

Vejamos de forma mais detalhada as etapas dos assistentes ao reverter alterações.

Step 1. Iniciando o Assistente

Selecione **Reverter alterações** e clique no botão **Avançar**.

Step 2. Pesquisa de alterações

O Assistente procura as alterações feitas anteriormente e que podem ser revertidas. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Step 3. Selecionar alterações que devem ser revertidas

Nesta etapa, é fornecido um relatório das alterações detectadas. O relatório é exibido como uma lista que inclui as ações do assistente que podem ser revertidas.

Para que o assistente reverta uma ação executada anteriormente, marque a caixa à esquerda do nome da ação.

Depois de criar o conjunto de ações que devem ser revertidas, clique no botão **Avançar**.

Step 4. Reversão de alterações

O assistente reverte as ações selecionadas na etapa anterior. Ao concluir a reversão de alterações, o Assistente continuará automaticamente na etapa seguinte.

Step 5. Conclusão do Assistente

Clique no botão **Concluir** para fechar o assistente.

RELATÓRIOS

Os eventos que ocorrem durante a operação dos componentes de proteção ou enquanto as tarefas do Kaspersky Anti-Virus são executadas são registrados em relatórios. Você pode criar um relatório detalhado para cada tarefa ou componente de proteção, além de configurar a exibição dos dados da forma mais conveniente. Além disso, é possível filtrar dados (consulte a seção "Filtragem de dados" na página 132) e pesquisar (consulte a seção "Pesquisa de eventos" na página 132) todos os eventos incluídos no relatório.

Se necessário, você pode salvar dados de relatório (consulte a seção "Salvando o relatório em arquivo" na página 133) em um arquivo de texto. Você também pode limpar os relatórios (consulte a seção "Limpando os relatórios do aplicativo" na página 134) que contêm dados que não são mais úteis, e ajustar as configurações de criação (consulte a seção "Registrando eventos não críticos" na página 134) e armazenamento (consulte a seção "Armazenando relatórios" na página 133) de relatórios.

NESTA SEÇÃO:

Criando um relatório para o componente selecionado 131

Filtragem de dados 132

Pesquisa de eventos 132

Salvando um relatório em arquivo 133

Armazenando relatórios 133

Limpando os relatórios do aplicativo 134

Registrando eventos não críticos 134

Configurando o lembrete de disponibilidade de relatórios 134

CRIANDO UM RELATÓRIO PARA O COMPONENTE SELECIONADO

Você pode obter um relatório completo dos eventos ocorridos durante a operação de cada componente do Kaspersky Anti-Virus ou durante a execução de suas tarefas.

Para trabalhar com os relatórios de forma conveniente, você pode alterar a exibição dos dados na tela: agrupar eventos por diversos parâmetros, selecionar o período do relatório, classificar eventos por coluna ou por importância, além de ocultar colunas.

Para criar um relatório sobre um determinado componente ou tarefa:

1. Abra a janela principal do aplicativo.
2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.
3. Na janela que é aberta, na guia **Relatório**, clique no botão **Relatório detalhado**.
4. À esquerda da janela **Relatório detalhado** que é aberta, selecione o componente ou a tarefa para o qual deve ser criado um relatório. Ao selecionar o item **Centro de Proteção**, é criado um relatório de todos os componentes de proteção.

FILTRAGEM DE DADOS

Você pode filtrar os eventos dos relatórios do Kaspersky Anti-Virus por um ou vários valores nas colunas do relatório, além de definir condições complexas de filtragem de dados.

Para filtrar eventos de acordo com seus valores:

1. Abra a janela principal do aplicativo.
2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.
3. Na janela que é aberta, na guia **Relatório**, clique no botão **Relatório detalhado**.
4. À direita da janela **Relatório detalhado** que é aberta, mova o ponteiro do mouse para o canto superior esquerdo do cabeçalho da coluna e clique nele para abrir o menu do filtro.
5. No menu do filtro, selecione o valor que deve ser usado para filtrar os dados.
6. Repita o procedimento para outra coluna, se necessário.

Para especificar uma condição de filtragem complexa:

1. Abra a janela principal do aplicativo.
2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.
3. Na janela que é aberta, na guia **Relatório**, clique no botão **Relatório detalhado**.
4. À direita da janela **Relatório detalhado** que é aberta, clique com o botão direito do mouse na coluna do relatório apropriada para exibir o menu de contexto e selecione **Filtrar**.
5. Na janela **Filtro personalizado** que é aberta, especifique as configurações de filtragem:
   a. Defina os limites da consulta à direita da janela.
   b. À esquerda da janela, na lista suspensa **Condição**, selecione as condições de consulta desejadas (por exemplo, é maior ou menor, igual ou diferente do valor especificado como limite de consulta).
   c. Se necessário, adicione uma segunda condição usando as operações lógicas de conjunção (AND lógico) ou disjunção (OR lógico). Se deseja que sua consulta de dados atenda às duas condições especificadas, selecione **E**. Se apenas uma das duas condições for necessária, selecione **OU**.

PESQUISA DE EVENTOS

Você pode pesquisar em um relatório o evento desejado usando uma palavra-chave na linha de pesquisa ou na janela de pesquisa especial.

Para localizar um evento usando a linha de pesquisa:

1. Abra a janela principal do aplicativo.
2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.
3. Na janela que é aberta, na guia **Relatório**, clique no botão **Relatório detalhado**.
4. Insira a palavra-chave na linha de pesquisa à direita da janela **Relatório detalhado** que é aberta.

Para localizar um evento usando a janela de pesquisa:

1. Abra a janela principal do aplicativo.
2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.
3. Na janela que é aberta, na guia **Relatório**, clique no botão **Relatório detalhado**.
4. À direita da janela **Relatório detalhado** que é aberta, clique com o botão direito do mouse no cabeçalho da coluna apropriada para exibir o menu de contexto correspondente e selecione **Pesquisar**.
5. Especifique os critérios de pesquisa na janela **Pesquisar** que é aberta:
   a. No campo **Texto**, insira uma palavra-chave para a pesquisa.
   b. Na lista suspensa **Coluna**, selecione o nome da coluna na qual deve ser pesquisada a palavra-chave especificada.
   c. Se necessário, marque as caixas correspondentes às configurações de pesquisa adicionais.
6. Clique no botão **Localizar próximo**.

SALVANDO UM RELATÓRIO EM ARQUIVO

O relatório obtido pode ser gravado em um arquivo de texto.

Para salvar o relatório em arquivo:

1. Abra a janela principal do aplicativo.
2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.
3. Na janela que é aberta, na guia **Relatório**, clique no botão **Relatório detalhado**.
4. Na janela **Relatório detalhado** que é aberta, crie o relatório desejado e clique no botão **Salvar**.
5. Na janela que é aberta, selecione a pasta na qual você deseja salvar o arquivo de relatório e insira o nome do arquivo.

ARMAZENANDO RELATÓRIOS

O período máximo de armazenamento de relatórios é de 30 dias. Depois disso, os relatórios são excluídos. Você pode cancelar a restrição de tempo ou alterar a duração máxima do armazenamento de relatórios.

Além disso, também é possível definir o tamanho máximo do tamanho dos relatórios. Por padrão, o tamanho máximo é 1024 MB. Quando ele for atingido, o conteúdo do arquivo será substituído por novos registros. Você pode cancelar os limites impostos sobre o tamanho do relatório ou inserir outro valor.

- *Para modificar o tempo máximo de armazenamento de relatórios:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
  3. À direita da janela, na seção **Armazenando relatórios**, marque a caixa **Armazenar relatórios por no máximo** e especifique o período máximo de armazenamento de relatórios.

- *Para configurar o tamanho máximo dos arquivos de relatório:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
  3. À direita da janela, na seção **Armazenando relatórios**, marque a caixa **Tamanho máximo de arquivo** e especifique o tamanho máximo dos arquivos de relatório.

LIMPANDO OS RELATÓRIOS DO APLICATIVO

Você pode limpar os relatórios que contêm dados dos quais você não precisa mais.

- *Para limpar os* relatórios:

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
  3. À direita da janela, na seção **Limpar relatórios**, clique no botão **Limpar**.
  4. Na janela **Limpando relatórios** que é aberta, marque as caixas dos relatórios que você deseja limpar.

REGISTRANDO EVENTOS NÃO CRÍTICOS

Por padrão, o produto não inclui em seus relatórios eventos não críticos, eventos do Registro e do sistema de arquivos. Você pode adicionar esses registros aos relatórios de proteção.

- *Para incluir uma entrada em um log de eventos não críticos:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
  3. À direita da janela, desmarque a caixa **Registrar eventos não-críticos**.

CONFIGURANDO O LEMBRETE DE DISPONIBILIDADE DE RELATÓRIOS

Você pode criar uma programação de acordo com a qual o Kaspersky Anti-Virus o lembrará sobre a disponibilidade de relatórios.

Para criar uma programação:

1. Abra a janela principal do aplicativo.

2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.

3. Na janela que é aberta, na guia **Relatório**, marque a caixa **Notificar sobre o relatório** e abra a janela de configurações da programação clicando no link com a configuração de hora.

4. Na janela **Programação de relatórios** que é aberta, especifique as configurações da programação.

EXIBIÇÃO DO APLICATIVO

Você pode alterar a aparência do Kaspersky Anti-Virus usando capas alternativas. Além disso, é possível configurar o uso dos elementos ativos da interface (como o ícone do aplicativo na área de notificação da barra de tarefas do Microsoft Windows ou as mensagens pop-up).

NESTA SEÇÃO:

Capa do aplicativo 135

Elementos ativos da interface 135

Agente de Notícias 135

CAPA DO APLICATIVO

É possível modificar todas as cores, fontes, ícones e textos usados na interface do Kaspersky Anti-Virus. Você pode criar suas próprias capas para o aplicativo ou traduzir a interface para outro idioma.

Para usar outra capa do aplicativo:

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Aparência**.

3. Marque a caixa **Usar capa alternativa** à direita da janela para ativar uma capa. Especifique a pasta com as configurações de capa no campo de entrada ou clique no botão **Procurar** para localizar o diretório.

ELEMENTOS ATIVOS DA INTERFACE

Você pode configurar a exibição de elementos ativos da interface, como janelas de notificação ou o ícone do Kaspersky Anti-Virus na barra de tarefas.

Para configurar os elementos ativos da interface:

1. Abra a janela de configurações do aplicativo.

2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Aparência**.

3. Na seção **Ícone na área de notificação da barra de tarefas**, marque ou desmarque as caixas desejadas.

AGENTE DE NOTÍCIAS

Através do *Agente de Notícias*, a Kaspersky Lab fornece informações sobre todos os eventos importantes relacionados ao Kaspersky Anti-Virus e à proteção geral contra ameaças de computador.

O aplicativo o notifica sobre as notícias mais recentes exibindo uma mensagem pop-up na área de notificações da barra de tarefas. Nesse caso, a forma do ícone do aplicativo é alterada (veja a seguir). Também são exibidas informações sobre o número de itens de notícias não lidos na janela principal do aplicativo. No menu de contexto do ícone do aplicativo, é exibido o item **Notícias**; enquanto isso, um ícone de notícias é exibido na interface do Kaspersky Anti-Virus Gadget.

Você pode ler as notícias das seguintes maneiras:

- clique no ícone na área de notificações da barra de tarefas;
- selecione **Notícias** no menu de contexto do ícone do aplicativo;
- clique no link **Ler as notícias** na mensagem pop-up de notícias;
- clique no link **Notícias** na janela principal do aplicativo;
- clique no ícone que aparece no centro do Gadget quando é exibida uma notícia (somente no Microsoft Windows Vista e no Microsoft Windows 7).

Os métodos listados acima para abrir a janela do Agente de Notícias estarão acessíveis somente se houver notícias não lidas disponíveis.

Se você não desejar receber notícias, poderá usar um dos seguintes métodos para desativar sua entrega:

- na janela do Agente de Notícias (somente se houver notícias não lidas disponíveis);
- na janela de configurações do aplicativo.

Para desativar a entrega de notícias na janela do Agente de Notícias:

1. Abra a janela do Agente de Notícias (veja as instruções acima).
2. Desmarque a caixa **Sempre receber notícias**.

Para desativar a entrega de notícias na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Aparência**.
3. Na seção **Ícone na área de notificação da barra de tarefas**, desmarque a caixa **Ativar notificações de notícias**.

NOTIFICAÇÕES

Por padrão, se ocorrerem eventos durante sua operação, o Kaspersky Anti-Virus o notificará. Se for necessário selecionar outras ações, serão exibidas janelas de notificação na tela (consulte a seção "Janelas de notificação e mensagens pop-up" na página 46). A encontrar eventos que não exigem a seleção de ações, o aplicativo o notifica usando sinais sonoros, emails e mensagens pop-up na área de notificação da barra de tarefas (consulte a seção "Janelas de notificação e mensagens pop-up" na página 46).

Você pode selecionar os métodos de notificação (consulte a seção "Configurando o método de notificação" na página 137) de eventos ou desativar as notificações (consulte a seção "Ativando e desativando as notificações" na página 137).

NESTA SEÇÃO:

Ativando e desativando as notificações 137

Configurando o método de notificação 137

ATIVANDO E DESATIVANDO AS NOTIFICAÇÕES

Por padrão, o Kaspersky Anti-Virus usa vários métodos para notificá-lo sobre todos os eventos importantes relacionados à operação do aplicativo (consulte a seção "Configurando o método de notificação" na página 137). É possível desativar a entrega de notificações.

Independentemente da entrega de notificações estar ativada ou desativada, as informações sobre eventos ocorridos durante a operação do Kaspersky Anti-Virus são registradas no relatório de operação do aplicativo.

A desativação da entrega de notificações não afeta a exibição das janelas de notificação. Para minimizar o número de janelas de notificação exibidas na tela, use o modo de proteção automática (consulte a seção "Selecionando o modo de proteção" na página 77).

Para desativar a entrega de notificações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, desmarque a caixa **Ativar notificações de eventos**.

CONFIGURANDO O MÉTODO DE NOTIFICAÇÃO

O aplicativo notifica sobre eventos usando os seguintes métodos:

- mensagens pop-up na área de notificação da barra de tarefas;
- notificações sonoras;
- mensagens por email.

Você pode configurar os métodos de entrega de um conjunto individual de notificações para cada tipo de evento.

Por padrão, as notificações críticas e de falhas de operação do aplicativo são acompanhadas de um sinal sonoro. O esquema de som do Microsoft Windows é usado como fonte dos efeitos sonoros. Você pode modificar o esquema atual ou desativar os sons.

Para configurar os métodos de entrega de notificações para diversos tipos de evento:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, marque a caixa **Ativar notificações de eventos** e clique no botão **Configurações** abaixo da caixa.
4. Na janela **Notificações** que é aberta, marque as caixas de acordo com a forma como deseja ser notificado sobre os diversos eventos: por email, através de mensagens pop-up ou por um sinal sonoro. Para evitar receber notificações sobre um determinado tipo de evento, desmarque todas as caixas na linha correspondente ao evento.

Para que o Kaspersky Anti-Virus o notifique sobre eventos por email, ajuste as configurações de entrega de notificações por email.

Para modificar as configurações de email para entrega de notificações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, marque a caixa **Ativar notificações por email** e clique no botão **Configurações**.
4. Na janela **Configurações de notificação por email** que é aberta, especifique as configurações de entrega.

Para modificar o esquema de som usado com as notificações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, marque a caixa **Usar esquema de som Padrão do Windows** e edite o esquema no sistema operacional.

   Se a caixa estiver desmarcada, será usado o esquema de som das versões anteriores do aplicativo.

Para desativar as notificações sonoras:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, desmarque a caixa **Ativar notificações sonoras**.

PARTICIPANDO DO KASPERSKY SECURITY NETWORK

Diariamente, aparece um grande número de novas ameaças em todo o mundo. Você pode se associar ao Kaspersky Security Network para acelerar a coleta de dados estatísticos cobre os tipos e fontes de novas ameaças, além de ajudar a desenvolver métodos para neutralizá-las.

O Kaspersky Security Network (KSN) é uma infraestrutura de serviços online que dá acesso à Base de Dados de Conhecimento online da Kaspersky Lab, que contém informações sobre a reputação de arquivos, recursos da Web e software. A utilização de dados do Kaspersky Security Network garante um tempo de resposta menor do Kaspersky Anti-Virus ao encontrar novos tipos de ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

Se você participar do Kaspersky Security Network, determinadas estatísticas coletadas no computador pelo Kaspersky Anti-Virus são enviadas automaticamente para a Kaspersky Lab.

Nenhum dado pessoal do usuário é coletado, processado ou armazenado.

A participação no Kaspersky Security Network é voluntária. Você pode decidir participar durante a instalação do Kaspersky Anti-Virus, mas isso pode ser alterado a qualquer momento.

Para ativar o Kaspersky Security Network:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Feedback**.
3. À direita da janela, marque a caixa **Concordo em participar do programa Kaspersky Security Network**.

VALIDANDO AS CONFIGURAÇÕES DO KASPERSKY ANTI-VIRUS

Depois que o Kaspersky Anti-Virus for instalado e configurado, você poderá verificar se a configuração está correta usando um "vírus" de teste e suas modificações. É necessário realizar um teste separado para cada componente/protocolo de proteção.

NESTA SEÇÃO:

O "vírus" de teste da EICAR e suas modificações 139

Testando a proteção do tráfego HTTP 140

Testando a proteção do tráfego SMTP 141

Validando as configurações do Antivírus de Arquivos 141

Validando as configurações da tarefa de verificação de vírus 142

Validando as configurações do Antispam 142

O "VÍRUS" DE TESTE DA EICAR E SUAS MODIFICAÇÕES

Este "vírus" de teste foi especialmente desenvolvido pela EICAR (The European Institute for Computer Antivirus Research) para testar produtos antivírus.

O "vírus" de teste NÃO É um vírus real, pois não contém nenhum código que possa danificar seu computador. Entretanto, a maioria dos produtos antivírus identifica o EICAR como um vírus.

Nunca use vírus reais para testar o funcionamento de um produto antivírus.

Você pode baixar este "vírus" de teste no site oficial da EICAR em http://www.eicar.org/anti_virus_test_file.htm.

Antes de baixar o arquivo, você deve pausar a proteção antivírus (consulte a seção "Pausando e reiniciando a proteção" na página 54) porque, caso contrário, o aplicativo identificaria e processaria o arquivo anti_virus_test_file.htm como um objeto infectado transferido por HTTP.

O aplicativo identifica o arquivo baixado do site da EICAR como um objeto infectado que contém um vírus que não pode ser desinfetado e executa as ações especificadas para este tipo de objeto.

Também é possível modificar o "vírus" de teste padrão para verificar a operação do aplicativo. Para modificar o "vírus", altere o conteúdo do "vírus" de teste padrão, adicionando um dos prefixos a ele (veja a tabela a seguir). Para modificar o "vírus" de teste, é possível usar qualquer editor de texto ou hipertexto, como o Bloco de Notas da Microsoft ou o UltraEdit32.

A primeira coluna da tabela (veja a seguir) contém os prefixos que devem ser adicionados ao início do "vírus" de teste padrão para criar suas modificações. A segunda coluna lista todos os status possíveis atribuídos ao objeto com base nos resultados da verificação executada pelo aplicativo. A terceira coluna indica como o aplicativo processa os objetos com o status especificado. As ações reais executadas com os objetos são determinadas pelas configurações do aplicativo.

Depois de ter adicionado o prefixo ao "vírus" de teste, salve o arquivo resultante com um nome que reflita a modificação do "vírus", por exemplo, depois de adicionar o prefixo DELE-, salve o arquivo como eicar_dele.com.

Verifique se você reiniciou a proteção antivírus depois de baixar o "vírus" de teste e criar suas modificações.

Table 2. Modificações do vírus de teste

Prefixo	Status do objeto	Informação sobre o processamento do objeto
Sem prefixo, "vírus" de teste padrão.	**Infectado**. O objeto contém o código de um vírus conhecido. Não é possível desinfetar.	O aplicativo identifica o objeto como um vírus que não pode se desinfetado. Ao tentar desinfetar o objeto, ocorre um erro; a ação executada será aquela especificada para objetos que não podem ser desinfetados.
CORR-	**Corrompido**.	O aplicativo pode acessar o objeto, mas não verificá-lo, pois ele está corrompido (por exemplo, a estrutura do arquivo está corrompida ou o formato do arquivo é inválido). Você pode encontrar informações de que o objeto foi processado no relatório de operação do aplicativo.
WARN-	**Suspeito**. O objeto contém o código de um vírus desconhecido. Não é possível desinfetar.	O objeto foi considerado suspeito. No momento da detecção, os bancos de dados do aplicativo não contêm nenhuma descrição do procedimento para desinfetar esse objeto. Você será notificado quando um objeto desse tipo for detectado.
SUSP-	**Suspeito**. O objeto contém o código modificado de um vírus conhecido. Não é possível desinfetar.	O aplicativo detectou uma correspondência parcial de uma seção do código do objeto com uma seção do código de um vírus conhecido. No momento da detecção, os bancos de dados do aplicativo não contêm nenhuma descrição do procedimento para desinfetar esse objeto. Você será notificado quando um objeto desse tipo for detectado.
ERRO-	**Erro de verificação**.	Ocorreu um erro durante a verificação de um objeto. O aplicativo não pode acessar o objeto, pois a integridade do mesmo foi violada (por exemplo, não existe um final em um arquivo comprimido com vários volumes) ou não é possível conectá-lo (se o objeto estiver sendo verificado em um recurso de rede). Você pode encontrar informações de que o objeto foi processado no relatório de operação do aplicativo.
CURE-	**Infectado**. O objeto contém o código de um vírus conhecido. Pode ser desinfetado.	O objeto contém um vírus que pode ser desinfetado. O aplicativo desinfetará o objeto; o texto do corpo do vírus será substituído pela palavra CURE. Você será notificado quando um objeto desse tipo for detectado.
DELE-	**Infectado**. O objeto contém o código de um vírus conhecido. Não é possível desinfetar.	O aplicativo identifica o objeto como um vírus que não pode se desinfetado. Ao tentar desinfetar o objeto, ocorre um erro; a ação executada será aquela especificada para objetos que não podem ser desinfetados. Você será notificado quando um objeto desse tipo for detectado.

TESTANDO A PROTEÇÃO DO TRÁFEGO HTTP

- *Para verificar se os vírus no fluxo de dados transferidos pelo protocolo HTTP são detectados com êxito:*

  Tente baixar este "vírus" de teste do site oficial da **EICAR** em http://www.eicar.org/anti_virus_test_file.htm.

Quando o computador tentar baixar o "vírus" de teste, o Kaspersky Anti-Virus detectará este objeto, o identificará como um objeto infectado que não pode ser desinfetado e executará a ação especificada nas configurações de verificação do tráfego HTTP para os objetos com esse status. Por padrão, ao tentar baixar o "vírus" de teste, a conexão com o site

será encerrada e o navegador exibirá uma mensagem informando que esse objeto está infectado com o vírus EICAR-Test-File.

TESTANDO A PROTEÇÃO DO TRÁFEGO SMTP

Para detectar vírus nos fluxos de dados transferidos usando o protocolo SMTP, é necessário usar um sistema de email que use esse protocolo para transferir dados.

É recomendável verificar a detecção de vírus em várias partes dos emails enviados: no corpo da mensagem e nos anexos. Use o arquivo do "vírus" de teste da EICAR para os testes (consulte a seção "O "vírus" de teste da EICAR e suas modificações" na página 139).

Para testar a detecção de vírus em fluxos de dados transferidos pelo protocolo SMTP:

1. Crie uma mensagem no formato de texto sem formatação usando um programa de email instalado no seu computador.

   A mensagem que contém o vírus de teste não será verificada se for criada no formato RTF ou HTML.

2. De acordo com a parte da mensagem na qual o aplicativo deve detectar o vírus:

   - para verificar a detecção do vírus no corpo da mensagem, adicione o texto do "vírus" de teste da EICAR padrão ou modificado ao início da mensagem;
   - para verificar a detecção do vírus em anexos, anexe à mensagem um arquivo que contém o "vírus" de teste da EICAR.

3. Envie a mensagem ao administrador.

O aplicativo detectará o objeto, o identificará como infectado e bloqueará a mensagem.

VALIDANDO AS CONFIGURAÇÕES DO ANTIVÍRUS DE ARQUIVOS

Para verificar se as configurações do Antivírus de Arquivos estão corretas:

1. Crie uma pasta no disco. Copie o "vírus" de teste baixado do site oficial da **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) nessa pasta, juntamente com todas as modificações do "vírus" de teste que você criou.

2. Todos os eventos devem ser registrados, de forma que o arquivo do relatório mantenha os dados de objetos corrompidos e objetos ignorados devido a erros.

3. Execute o "vírus" de teste ou alguma de suas versões modificadas.

O componente Antivírus de Arquivos interceptará a chamada de execução do arquivo, o verificará e executará a ação especificada nas configurações para objetos com esse status. Ao selecionar ações diferentes a serem realizadas com o objeto detectado, você poderá executar uma verificação completa da operação do componente.

É possível exibir as informações sobre os resultados da operação do componente Antivírus de Arquivos no relatório de operação do componente.

VALIDANDO AS CONFIGURAÇÕES DA TAREFA DE VERIFICAÇÃO DE VÍRUS

Para verificar se as configurações da tarefa de verificação de vírus estão corretas:

1. Crie uma pasta no disco. Copie o "vírus" de teste baixado do site oficial da **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) nessa pasta, juntamente com todas as modificações do "vírus" de teste que você criou.

2. Crie uma nova tarefa de verificação de vírus e selecione a pasta que contém o conjunto de "vírus" de teste como o objeto a ser verificado.

3. Todos os eventos devem ser registrados, de forma que o arquivo do relatório mantenha os dados de objetos corrompidos e objetos ignorados devido a erros.

4. Execute a tarefa de verificação de vírus.

Ao executar a tarefa de verificação, as ações especificadas nas configurações de tarefa serão realizadas conforme objetos suspeitos ou infectados sejam detectados. Ao selecionar ações diferentes a serem realizadas com o objeto detectado, você poderá executar uma verificação completa da operação do componente.

É possível exibir todas as informações sobre as ações da tarefa de verificação de vírus no relatório de operação do componente.

VALIDANDO AS CONFIGURAÇÕES DO ANTISPAM

Você pode usar uma mensagem de teste identificada como SPAM, para testar a proteção antispam.

O corpo da mensagem de teste deve conter a seguinte frase:

```
Não envie spam, pois não é legal
```

Quando essa mensagem for recebida no computador, o Kaspersky Anti-Virus a verificará, atribuirá o status de "spam" a ela e executará a ação especificada para objetos desse tipo.

ENTRANDO EM CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO

Se houver problemas durante a operação do Kaspersky Anti-Virus, primeiro verifique se o método para solucioná-los está descrito na documentação, na ajuda, no Banco de Dados de Conhecimento no site de Suporte Técnico ou no Fórum de Usuários da Kaspersky Lab.

Se você não conseguir encontrar uma solução para o problema, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab de uma das seguintes maneiras:

- envie uma consulta através do Gabinete Pessoal no site do Serviço de Suporte Técnico;
- por telefone.

Os especialistas do Serviço de Suporte Técnico responderão todas as suas dúvidas sobre a instalação, a ativação e o uso do aplicativo. Eles ajudarão a eliminar as consequências das atividades de malware, caso seu computador tenha sido infectado.

Antes de entrar em contato com o serviço de Suporte técnico, leia as regras de Suporte para os produtos da Kaspersky Lab (http://support.kaspersky.com/support/rules).

Ao entrar em contato com o Serviço de Suporte Técnico, os especialistas do serviço podem solicitar que você compile um relatório do status do sistema e um arquivo de rastreamento para enviar a eles. Depois que os especialistas do Serviço de Suporte Técnico analisarem os dados que você enviou, eles poderão criar um script do AVZ para ajudar a eliminar os seus problemas.

NESTA SEÇÃO:

Minha conta Kaspersky 143

Suporte técnico por telefone 144

Criando um relatório de estado do sistema 144

Criando um arquivo de rastreamento 145

Enviando arquivos de dados 145

Execução do script do AVZ 146

MINHA CONTA KASPERSKY

Minha conta Kaspersky – sua seção pessoal no site do Serviço de Suporte Técnico. Ao usar a Minha conta Kaspersky, você pode executar as seguintes ações:

- entrar em contato com o Serviço de Suporte Técnico e o Laboratório de Vírus;
- entrar em contato com o Serviço de Suporte Técnico sem usar o email;
- rastrear o status das suas solicitações em tempo real;
- exibir um histórico detalhado de suas solicitações para o Serviço de Suporte Técnico.

Para entrar na Minha conta Kaspersky, use uma das seguintes opções:

- clique no link **Minha conta Kaspersky** na janela principal do Kaspersky Anti-Virus;
- na barra de endereços do navegador, digite https://my.kaspersky.com.

Se você ainda não tiver uma conta, é possível se inscrever na página de registro da Minha Conta Kaspersky https://my.kaspersky.com/registration. Insira seu endereço de email e uma senha para entrar na Minha conta Kaspersky. Para enviar uma solicitação referente ao uso do Kaspersky Anti-Virus, será solicitado que você insira um código de ativação.

Algumas solicitações não devem ser endereçadas ao Serviço de Suporte Técnico, mas ao Laboratório de Vírus da Kaspersky. Essas solicitações são as dos seguintes tipos:

- programa malicioso desconhecido – você suspeita que um objeto é malicioso, embora o Kaspersky Anti-Virus não o classifique assim;
- falso positivo – o Kaspersky Anti-Virus classifica um arquivo como vírus, mas você tem certeza de que o arquivo é íntegro;
- descrição do programa malicioso – você deseja obter a descrição de um vírus específico.

Para enviar uma solicitação ao Laboratório de Vírus, não é necessário inserir um código de ativação.

Não é necessário ser usuário registrado da Minha Conta Kaspersky para enviar solicitações ao Laboratório de Vírus da página com o formulário de solicitação (http://support.kaspersky.com/virlab/helpdesk.html).

SUPORTE TÉCNICO POR TELEFONE

Ao encontrar algum problema que exija ajuda urgente, você pode ligar para o Suporte Técnico. Antes de ligar para os especialistas em suporte técnico na Região (http://brazil.kaspersky.com/suporte/informa%C3%A7%C3%B5es-de-contato-do-suporte-para-usu%C3%A1rios-dom%C3%A9sticos), tenha em mãos as informações (http://support.kaspersky.com/support/details) sobre o seu computador e o aplicativo antivírus instalado nele. Assim, nossos especialistas poderão ajudá-lo mais rapidamente.

CRIANDO UM RELATÓRIO DE ESTADO DO SISTEMA

Para solucionar seus problemas, os especialistas do Serviço de Suporte Técnico da Kaspersky Lab podem solicitar um relatório sobre o estado do sistema. Esse relatório contém informações detalhadas sobre os processos em execução, os módulos e drivers carregados, os plug-ins do Microsoft Internet Explorer e do Microsoft Windows Explorer, as portas abertas, os objetos suspeitos detectados, etc.

Ao criar um relatório de estado do sistema, nenhuma informação pessoal do usuário é coletada.

Para criar um relatório de estado do sistema:

1. Abra a janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).
2. Use o link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de suporte**.
3. Na janela **Informações para o Serviço de Suporte Técnico** que é aberta, clique no botão **Criar relatório de estado do sistema**.

O relatório de estado do sistema é criado nos formatos HTML e XML e é salvo no arquivo comprimido sysinfo.zip. Quando as informações tiverem sido coletadas, você poderá exibir o relatório.

Para exibir o relatório:

1. Abra a janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).
2. Use o link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de suporte**.
3. Na janela **Informações para o Serviço de Suporte Técnico** que é aberta, clique no botão **Exibir**.
4. Abra o arquivo comprimido sysinfo.zip, que contém arquivos de relatório.

CRIANDO UM ARQUIVO DE RASTREAMENTO

Depois de instalar o Kaspersky Anti-Virus, podem ocorrer algumas falhas no sistema operacional ou na operação de aplicativos individuais. A causa mais provável é um conflito entre o Kaspersky Anti-Virus e o software instalado no computador, ou com os drivers dos componentes do computador. Talvez seja solicitado que você crie um arquivo de rastreamento para que os especialistas do Serviço de Suporte Técnico da Kaspersky Lab possam solucionar seu problema.

Para criar o arquivo de rastreamento:

1. Abra a janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).
2. Use o link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de suporte**.
3. Na janela **Informações para o Serviço de Suporte Técnico** que é aberta, especifique o nível de rastreamento na lista suspensa da seção **Rastros**.

   É recomendável esclarecer o nível de rastreamento desejado com um especialista do Serviço de Suporte Técnico. Quando não houver orientação do Serviço de Suporte Técnico, é recomendável definir o nível de rastreamento como **500**.
4. Para iniciar o processo de rastreamento, clique no botão **Ativar**.
5. Reconstrua a situação em que o problema ocorreu.
6. Para interromper o processo de rastreamento, clique no botão **Desativar**.

Você pode alternar para o carregamento de resultados de rastreamento (consulte a seção "Enviando arquivos de dados" na página 145) em um servidor da Kaspersky Lab.

ENVIANDO ARQUIVOS DE DADOS

Depois de criar os arquivos de rastreamento e o relatório de estado do sistema, você deverá enviá-los aos especialistas do Serviço de Suporte Técnico da Kaspersky Lab.

Você precisará de um número de solicitação para carregar os arquivos de dados no servidor do Serviço de Suporte Técnico. Esse número está disponível no seu Gabinete Pessoal no site do Serviço Suporte Técnico, se a sua solicitação estiver ativa.

Para carregar os arquivos de dados no servidor do Serviço de Suporte Técnico:

1. Abra a janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).
2. Use o link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de suporte**.

3. Na janela **Informações para o Serviço de Suporte Técnico** que é aberta, na seção **Ações**, clique no botão **Carregar informações para o serviço de Suporte técnico no servidor**.

   A janela **Carregando informações no servidor para o Serviço de Suporte Técnico** será aberta.

4. Marque as caixas ao lado dos arquivos de rastreamento que você deseja enviar ao Serviço de Suporte Técnico e clique no botão **Enviar**.

   O **Número da solicitação** é aberto.

5. Especifique o número atribuído à sua solicitação entrando em contato com o Serviço de Suporte Técnico através da Minha Conta Kaspersky e clique no botão **OK**.

Os arquivos de dados selecionados são compactados e enviados ao servidor do Serviço de Suporte Técnico.

Se, por algum motivo, não for possível entrar em contato com o Serviço de Suporte Técnico, os arquivos de dados poderão ser armazenados no seu computador e enviados posteriormente a partir do Gabinete Pessoal.

Para salvar os arquivos de dados em disco:

1. Abra a janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).

2. Use o link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de suporte**.

3. Na janela **Informações para o Serviço de Suporte Técnico** que é aberta, na seção **Ações**, clique no botão **Carregar informações para o serviço de Suporte técnico no servidor**.

   A janela **Carregando informações no servidor para o Serviço de Suporte Técnico** será aberta.

4. Marque as caixas ao lado dos arquivos de rastreamento que você deseja enviar ao Serviço de Suporte Técnico e clique no botão **Enviar**.

   O **Número da solicitação** é aberto.

5. Clique no botão **Cancelar** e, na janela que é aberta, confirme a gravação dos arquivos em disco clicando no botão **Sim**.

   A janela para gravação do arquivo comprimido será aberta.

6. Especifique o nome do arquivo comprimido e confirme a gravação.

O arquivo comprimido criado pode ser enviado ao Serviço de Suporte Técnico a partir do Gabinete Pessoal.

EXECUÇÃO DO SCRIPT DO AVZ

Os especialistas da Kaspersky Lab analisarão o problema usando os arquivos de rastreamento e o relatório de estado do sistema. O resultado da análise é uma sequência de ações para eliminar os problemas detectados. O número dessas ações pode ser bastante grande.

Para simplificar o procedimento, são usados scripts do AVZ. Um script do AVZ consiste em um conjunto de instruções que permite editar as chaves do registro, colocar arquivos na Quarentena, procurar classes de arquivos e arquivos possivelmente infectados relacionados a elas, bloquear os interceptadores no modo de usuário e modo kernel, etc.

Para executar scripts, o aplicativo inclui um *Assistente de Execução do Script do AVZ*.

O Assistente consiste em uma série de telas (etapas) nas quais você navega usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Não é recomendável alterar o texto de um script do AVZ recebido dos especialistas da Kaspersky Lab. Se houver problemas durante a execução do script, entre em contato com o Serviço de Suporte Técnico.

Para iniciar o Assistente:

1. Abra a janela principal do aplicativo (consulte a seção "Janela principal do Kaspersky Anti-Virus" na página 44).
2. Use o link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de suporte**.
3. Na janela **Informações para o Serviço de Suporte Técnico** que é aberta, clique no botão **Executar script do AVZ**.

Se o script for executado com êxito, o Assistente será fechado. Se ocorrer um erro durante a execução do script, o Assistente exibirá uma mensagem de erro correspondente.

APÊNDICE

Esta seção inclui informações de referência que complementam o texto da documentação.

NESTA SEÇÃO:

Status da assinatura 148

Lista de notificações do Kaspersky Anti-Virus..... 150

Trabalhando com o aplicativo na linha de comando 164

STATUS DA ASSINATURA

As seguintes opções são usadas para definir o status da assinatura:

- *Em definição*. Sua solicitação de ativação da assinatura ainda não foi processada (é necessário um tempo para o processamento da solicitação no servidor). O Kaspersky Anti-Virus trabalha no modo totalmente funcional. Se, após um determinado período, a solicitação da assinatura ainda não tiver sido processada, você receberá uma notificação de que a atualização do status da assinatura não foi realizada. Nesse caso, os bancos de dados do aplicativo não serão mais atualizados (para a licença com assinatura de atualização) e a proteção do computador não será executada (para a licença com assinatura de proteção e atualização).

- *Ativo*. A assinatura foi ativada sem um período fixo ou por um determinado período (a data de expiração da assinatura foi definida).

- *Renovada*. A assinatura foi renovada sem um período fixo ou por um determinado período.

- *Erro*. Ocorreu um erro ao atualizar o status da assinatura.

- *Expirada. Período de tolerância.* A assinatura ou o período de renovação do status expirou. Se o período de renovação do status tiver expirado, atualize o status da assinatura manualmente. Se a assinatura tiver expirado, você poderá renová-la entrando em contato com a loja virtual na qual você comprou o Kaspersky Anti-Virus. Para usar outro código de ativação, primeiro exclua o arquivo da chave da assinatura em uso no momento.

- *Expirada. Período de tolerância expirado.* A assinatura ou o período de tolerância de renovação da licença expirou. Entre em contato com seu provedor de assinaturas para comprar uma nova assinatura ou para renovar a assinatura existente.

  Se o período de validade da assinatura tiver terminado, assim como o período de tolerância durante o qual a licença pode ser renovada (status da assinatura – *Expirada*), o Kaspersky Anti-Virus o notificará e interromperá as tentativas de renovar a licença automaticamente. Para a licença com assinatura de atualização, a funcionalidade do aplicativo será mantida, exceto pelo recurso de atualização dos bancos de dados. Para a licença com assinatura de proteção e atualização, os bancos de dados do aplicativo não serão atualizados, a proteção do computador e as tarefas de verificação não serão executadas.

- *Cancelamento da assinatura.* Você cancelou a assinatura da renovação automática da licença.

- *Atualização necessária*. Por algum motivo, o status da assinatura não foi atualizado no momento apropriado.

  Se a assinatura não foi renovada no momento correto (por exemplo, o computador estava desligado quando a renovação da licença estava disponível), é possível atualizar seu status manualmente na janela gerenciamento de licenças (consulte a seção "Exibindo informações da licença" na página 40). Até o momento da renovação da assinatura, o Kaspersky Anti-Virus interrompe a atualização dos bancos de dados do aplicativo (para a licença com assinatura de atualização) e interrompe a proteção do computador e a execução das tarefas de verificação (para a licença com assinatura de proteção).

- *Suspensa*. A assinatura da renovação automática da licença foi suspensa.

- *Reiniciada*. A assinatura foi reiniciada.

Em alguns casos, é possível exibir informações adicionais sobre o status da assinatura para uma licença com assinatura.

LISTA DE NOTIFICAÇÕES DO KASPERSKY ANTI-VIRUS

Esta seção contém a lista de notificações que podem ser exibidas na tela pelo Kaspersky Anti-Virus.

NESTA SEÇÃO:

Notificações em qualquer modo de proteção 150

Notificações no modo de proteção interativa 155

NOTIFICAÇÕES EM QUALQUER MODO DE PROTEÇÃO

Esta seção contém a lista de notificações que podem ser exibidas na tela no modo de proteção automática e no modo de proteção interativa (consulte a seção "Selecionando o modo de proteção" na página 77). Se desejar exibir todas as notificações disponíveis, alterne para o modo de proteção interativa. Nesse caso, além das notificações descritas nesta seção, também serão exibidas na tela as notificações exibidas somente no modo de proteção interativa (consulte a seção "Notificações no modo de proteção interativa" na página 155).

NESTA SEÇÃO:

Neutralização especial necessária 150

Unidade removível conectada 151

Nova rede detectada 151

Certificado não confiável detectado 152

Aplicativo possivelmente perigoso detectado 152

Arquivo da Quarentena não infectado 153

Lançamento de nova versão do produto 153

Lançamento de atualização técnica 153

Atualização técnica baixada 154

Atualização técnica baixada não instalada 154

Licença expirada 155

NEUTRALIZAÇÃO ESPECIAL NECESSÁRIA

Ao detectar uma ameaça ativa no sistema (por exemplo, um processo malicioso na RAM ou em objetos de inicialização), será exibida uma mensagem pop-up solicitando que você execute um procedimento especial de desinfecção avançada.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

O ícone é exibido ao lado do nome do objeto malicioso. Clique nele para abrir a janela com informações sobre o objeto. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.

- Nome do arquivo do objeto malicioso, incluindo seu caminho.

É solicitado que você selecione uma das seguintes ações:

- **Sim, desinfetar ao reiniciar** – executa o procedimento de desinfecção especial.

  Os especialistas da Kaspersky Lab recomendam enfaticamente que você selecione esta opção. No entanto, o sistema operacional será reiniciado após a conclusão do procedimento de desinfecção; assim, é recomendável salvar os resultados da atividade atual e fechar todos os aplicativos antes de executá-lo. Durante a desinfecção, todos os aplicativos são bloqueados, exceto os confiáveis. Depois de reiniciar o computador, é recomendável executar uma verificação completa de vírus.

- **Não executar** – o objeto ou o processo detectado será processado de acordo com a ação selecionada.

Para aplicar a ação selecionada sempre que esse evento ocorrer novamente, marque a caixa **Aplicar para todos os objetos**.

UNIDADE REMOVÍVEL CONECTADA

Quando uma unidade removível é conectada ao computador, a notificação é exibida na tela. É solicitado que você selecione uma das seguintes ações:

- **Verificação Rápida** – verifica apenas os arquivos armazenados na unidade removível que podem representar uma possível ameaça.

- **Verificação Completa** – verifica todos os arquivos armazenados na unidade removível.

- **Não verificar** – não verifica a unidade removível.

Para aplicar a ação selecionada a todas as unidades removíveis que podem ser conectadas no futuro, marque a caixa **Nesses casos, sempre executar**.

NOVA REDE DETECTADA

Sempre que o computador se conectar a uma nova zona (ou seja, uma rede), será exibida uma notificação pop-up.

A parte superior da notificação fornece informações sobre a rede:

- adaptador de rede usado para a conexão;

- tipo de rede (por exemplo, "sem fio");

- nome da rede.

A parte inferior da janela solicita que você atribua um status à zona; a atividade de rede será permitida de acordo com esse status:

- **Sim, é uma rede confiável**. Este status é recomendado apenas para zonas que, na sua opinião, são absolutamente seguras e que seu computador não estará sujeito a ataques ou tentativas de obter acesso aos seus dados.

- **Rede local**. Este status é recomendado para zonas com um fator de risco médio (por exemplo, redes corporativas).

- **Não, é uma rede pública**. Uma rede de alto risco, na qual o computador está em perigo de qualquer tipo possível de ameaça. É recomendável selecionar esse status para redes não protegidas por nenhum aplicativo

antivírus, firewall, filtro, etc. Ao selecionar esse status, o programa garante a segurança máxima para essa zona.

CERTIFICADO NÃO CONFIÁVEL DETECTADO

Uma verificação de segurança da conexão através do protocolo SSL é executada usando o certificado instalado. Se um certificado inválido for detectado ao tentar a conexão com o servidor (por exemplo, se o certificado for substituído por um invasor), será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- descrição da ameaça;
- link para exibir o certificado;
- causas prováveis do erro;
- URL do recurso da Web.

É solicitado que você decida se deve ser estabelecida uma conexão de rede com o certificado não confiável:

- **Sim, aceitar o certificado não confiável** – dá prosseguimento à conexão com o recurso da Web.
- **Negar o certificado** – interrompe a conexão com o site.

APLICATIVO POSSIVELMENTE PERIGOSO DETECTADO

Quando o Monitor de atividades detecta um aplicativo cujo comportamento é semelhante ao de malware, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo e nome do aplicativo possivelmente perigoso.

  O ícone é exibido ao lado do nome do aplicativo. Clique nele para abrir a janela com informações sobre o aplicativo.
- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.
- Link para a janela com o log de emergência do aplicativo.

Você pode selecionar uma das seguintes ações:

- **Quarentena** – fecha o aplicativo e move o arquivo do aplicativo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status de *não infectado* e ele pode ser restaurado.

  Se você mover manualmente para a Quarentena um arquivo que na verificação seguinte é classificado como não infectado, seu status será alterado para *OK* somente se ele tiver sido verificado por três dias depois de ter sido movido para a Quarentena, ou depois disso.
- **Encerrar** – interrompe a execução do aplicativo.
- **Permitir** – permite a execução do aplicativo.

- **Adicionar às exclusões** – permite que o aplicativo execute essas ações a qualquer momento no futuro.

ARQUIVO DA QUARENTENA NÃO INFECTADO

Por padrão, o Kaspersky Anti-Virus verifica os arquivos em quarentena após cada atualização dos bancos de dados. Se a verificação de um arquivo da Quarentena mostrar definitivamente que ele não está infectado, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- recomendação de restauração do arquivo da Quarentena;
- nome do arquivo, incluindo o caminho da pasta na qual ele foi armazenado antes de ser movido para a Quarentena.

É solicitado que você selecione uma das seguintes ações:

- **Restaurar** – restaura o arquivo, removendo-o da Quarentena para a pasta na qual ele foi armazenado antes de ser movido para a Quarentena.
- **Cancelar** – deixa o arquivo na Quarentena.

LANÇAMENTO DE NOVA VERSÃO DO PRODUTO

Quando uma nova versão do Kaspersky Anti-Virus é lançada, tornando-se disponível para download nos servidores da Kaspersky Lab, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- link para a janela com informações detalhadas sobre a versão recém-lançada do aplicativo;
- tamanho do pacote de instalação.

É solicitado que você selecione uma das seguintes ações:

- **Sim, baixar** – baixa o pacote de instalação da nova versão do aplicativo na pasta selecionada.
- **Não** – cancela o download do pacote de instalação.

Se você não desejar que a notificação sobre novas versões do aplicativo seja exibida na tela no futuro, marque a caixa **Não lembrar-me dessa atualização**.

LANÇAMENTO DE ATUALIZAÇÃO TÉCNICA

Quando uma atualização técnica do Kaspersky Anti-Virus é lançada, tornando-se disponível para download nos servidores da Kaspersky Lab, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- número da versão do aplicativo instalada no computador;
- número da versão do aplicativo após a atualização técnica esperada;
- link para a janela com informações detalhadas sobre a atualização técnica;
- tamanho do arquivo de atualização.

É solicitado que você selecione uma das seguintes ações:

- **Sim, baixar** – baixa o arquivo de atualização na pasta selecionada.
- **Não** – cancela o download da atualização. Esta opção estará disponível se a caixa **Não lembrar-me dessa atualização** estiver marcada (veja a seguir).
- **Não, lembre-me mais tarde** – cancela o download imediato e recebe uma notificação da atualização posteriormente. Esta opção estará disponível se a caixa **Não lembrar-me dessa atualização** estiver desmarcada (veja a seguir).

Se você não desejar que a notificação sobre novas versões do aplicativo seja exibida na tela no futuro, marque a caixa **Não lembrar-me dessa atualização**.

ATUALIZAÇÃO TÉCNICA BAIXADA

Quando o download da atualização técnica do Kaspersky Anti-Virus dos servidores da Kaspersky Lab for concluído, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- número da versão do aplicativo após a atualização técnica;
- link para o arquivo de atualização.

É solicitado que você selecione uma das seguintes ações:

- **Sim, instalar** – instala a atualização.

  Depois que a atualização for instalada, será necessário reiniciar o sistema operacional.

- **Adiar instalação** – cancela a instalação para executá-la posteriormente.

ATUALIZAÇÃO TÉCNICA BAIXADA NÃO INSTALADA

Quando uma atualização técnica do Kaspersky Anti-Virus é baixado mas não é instalado no computador, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- número da versão do aplicativo após a atualização técnica;
- link para o arquivo de atualização.

É solicitado que você selecione uma das seguintes ações:

- **Sim, instalar** – instala a atualização.

  Depois que a atualização for instalada, será necessário reiniciar o sistema operacional.

- **Adiar instalação** – cancela a instalação para executá-la posteriormente.

Se você não desejar que a notificação sobre esta atualização seja exibida na tela no futuro, marque a caixa **Não perguntar até que haja uma nova versão disponível**.

LICENÇA EXPIRADA

Quando a licença de avaliação expirar, o Kaspersky Anti-Virus exibirá uma notificação na tela.

A notificação fornece as seguintes informações:

- duração do período de avaliação;
- informações sobre o resultado da operação do aplicativo (pode incluir um link para obter mais detalhes).

É solicitado que você selecione uma das seguintes ações:

- **Sim, comprar** – esta opção abre a janela do navegador e carrega a página da Loja Virtual, na qual é possível comprar a licença comercial.
- **Cancelar** – rejeita o uso do aplicativo. Se você selecionar esta opção, o aplicativo interromperá a execução de todas as suas funções principais (verificação de vírus, atualização, proteção em tempo real).

NOTIFICAÇÕES NO MODO DE PROTEÇÃO INTERATIVA

Esta seção contém uma lista de notificações que são exibidas somente quando o aplicativo é executado no modo de proteção interativa (consulte a seção "Selecionando o modo de proteção" na página 77). Se você não desejar que essas notificações sejam exibidas na tela, alterne a proteção para o modo automático. Nesse caso, serão exibidas somente as notificações que são exibidas em qualquer modo de proteção (consulte a seção "Notificações em qualquer modo de proteção" na página 150).

NESTA SEÇÃO:

Atividade de rede de um aplicativo detectada 156

Objeto malicioso detectado 156

Vulnerabilidade detectada 157

Atividade perigosa detectada no sistema 158

Revertendo as alterações feitas por um aplicativo perigoso 158

Aplicativo malicioso detectado 159

Aplicativo malicioso ou aplicativo legal que pode ser usado por invasores detectado 159

Link suspeito/malicioso detectado 160

Objeto perigoso detectado no tráfego 160

Tentativa de acesso a um site de phishing detectada 162

Tentativa de acesso ao Registro do sistema detectada 162

O objeto não pode ser desinfetado 162

Processo oculto detectado 163

ATIVIDADE DE REDE DE UM APLICATIVO DETECTADA

Se for detectada qualquer atividade de rede de um aplicativo (opção padrão para os aplicativos dos grupos **Baixa Restrição** ou **Alta Restrição**), será exibida uma notificação na tela.

A notificação será exibida se o Kaspersky Anti-Virus for executado no modo interativo (consulte a seção "Selecionando o modo de proteção" na página 77) e se não tiver sido criada nenhuma regra de pacotes para o aplicativo cuja atividade de rede foi detectada.

A notificação contém as seguintes informações:

- nome do aplicativo e breve descrição da conexão iniciada por ele;
- informações sobre a conexão (tipo, local e porta remota da conexão, endereço com o qual a conexão é estabelecida);
- sequência de execução de aplicativos.

É solicitado que você selecione uma das seguintes ações:

- **Permitir agora**.
- **Bloquear agora**.
- **Criar uma regra**. Quando esta opção está selecionada, a janela **Firewall** é aberta e você pode criar uma regra para definir a atividade de rede do aplicativo.

Você pode bloquear ou permitir a atividade de rede do aplicativo uma vez ou por um período mais longo. Para fazer isso, execute uma das seguintes ações:

- Para bloquear ou permitir a atividade de rede de um aplicativo uma vez, selecione **Permitir agora** ou **Bloquear agora**.
- Para lembrar a ação selecionada durante toda a seção de um aplicativo que apresentou atividade de rede, selecione **Permitir agora** ou **Bloquear agora** e marque a caixa **Aplicar à sessão atual do aplicativo**.

  Se a caixa **Aplicar sempre** for exibida na janela, marque-a e clique no link **sempre** para alterar seu nome para **Aplicar à sessão atual do aplicativo**.
- Para sempre lembrar a ação selecionada para um aplicativo, selecione **Permitir agora** ou **Bloquear agora** e marque a caixa **Aplicar sempre**.

  Se a caixa **Aplicar à sessão atual do aplicativo** for exibida na janela, marque-a e clique no link **à sessão atual do aplicativo** para alterar seu nome para **Aplicar sempre**.

OBJETO MALICIOSO DETECTADO

Se o Antivírus de Arquivos, o Antivírus de Email ou uma verificação de vírus detectar um código malicioso, será exibida uma notificação pop-up.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto malicioso. Clique nele para abrir a janela com informações sobre o objeto. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.

- Nome do arquivo do objeto malicioso, incluindo seu caminho.

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Desinfetar** – tenta desinfetar o objeto malicioso. Esta opção estará disponível se a ameaça já for conhecida e o aplicativo puder tentar desinfetar o objeto.

  Antes da neutralização, é criada uma cópia de backup do objeto, caso seja necessário restaurá-lo ou descobrir como ele foi infectado.

- **Quarentena** – move o objeto para a Quarentena, onde ele não representa uma ameaça ao computador. Esta opção estará disponível se a ameaça for desconhecida e nenhum dos métodos de desinfecção existentes puder ser aplicado ao objeto.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status de *não infectado* e ele pode ser restaurado.

  Se você mover manualmente para a Quarentena um arquivo que na verificação seguinte é classificado como não infectado, seu status será alterado para *OK* somente se ele tiver sido verificado por três dias depois de ter sido movido para a Quarentena, ou depois disso.

- **Excluir** – exclui o objeto. Antes da exclusão, é criada uma cópia de backup do objeto para que ele possa ser restaurado posteriormente ou para poder rastrear a forma de infecção.

- **Ignorar/Bloquear** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Você pode retornar ao processamento de objetos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar para todos os objetos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o aplicativo ser reiniciado, ou o período entre o início e a conclusão de uma verificação de vírus.

VULNERABILIDADE DETECTADA

Se for detectada uma vulnerabilidade ao executar uma tarefa de verificação de vírus, será exibida uma notificação na tela.

Ela contém as seguintes informações:

- Descrições da vulnerabilidade.

- O nome da vulnerabilidade conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome. Clique nele para abrir a janela com informações sobre a vulnerabilidade. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a vulnerabilidade.

- Nome do arquivo do objeto vulnerável, incluindo seu caminho.

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Sim, corrigir** – elimina a vulnerabilidade.

- **Ignorar** – não executa nenhuma ação com o objeto vulnerável.

ATIVIDADE PERIGOSA DETECTADA NO SISTEMA

Quando a Defesa Proativa detecta a atividade perigosa de um aplicativo no sistema, é exibida uma notificação pop-up.

A notificação contém as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto malicioso. Clique nele para abrir a janela com informações sobre o objeto. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.
- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Quarentena** – fecha o aplicativo e move o arquivo do aplicativo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status de *não infectado* e ele pode ser restaurado.

  Se você mover manualmente para a Quarentena um arquivo que na verificação seguinte é classificado como não infectado, seu status será alterado para *OK* somente se ele tiver sido verificado por três dias depois de ter sido movido para a Quarentena, ou depois disso.
- **Encerrar** – interrompe a execução do aplicativo.
- **Permitir** – permite a execução do aplicativo.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual da Defesa Proativa, marque a caixa **Nesses casos, sempre executar**. A sessão atual do aplicativo consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou reiniciado.

Se tiver certeza de que o programa detectado não é perigoso, é recomendável adicioná-lo à zona confiável, para evitar que o Kaspersky Anti-Virus repita falsos positivos ao detectá-lo.

REVERTENDO AS ALTERAÇÕES FEITAS POR UM APLICATIVO PERIGOSO

Quando a execução de um aplicativo possivelmente perigoso é concluída, é recomendável reverter (cancelar) as alterações que ele fez no sistema. Nesse caso, uma notificação com uma solicitação de reversão das alterações é exibida na tela.

A notificação fornece as seguintes informações:

- Solicitação de reversão das alterações feitas por um aplicativo possivelmente perigoso.
- Tipo e nome do aplicativo.

  O ícone é exibido ao lado do nome do aplicativo. Clique nele para abrir a janela com informações sobre o aplicativo.
- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Sim, reverter** – tenta reverter as alterações feitas pelo aplicativo.

- **Ignorar** – cancela a reversão de alterações.

APLICATIVO MALICIOSO DETECTADO

Quando o Inspetor do Sistema detecta um aplicativo cujo comportamento corresponde inteiramente às atividades de aplicativos maliciosos, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo e nome do aplicativo malicioso.

  O ícone é exibido ao lado do nome do aplicativo. Clique nele para abrir a janela com informações sobre o aplicativo.
- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.
- Link para a janela com o log de emergência do aplicativo.

Você pode selecionar uma das seguintes ações:

- **Quarentena** – fecha o aplicativo e move o arquivo do aplicativo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status de *não infectado* e ele pode ser restaurado.

  Se você mover manualmente para a Quarentena um arquivo que na verificação seguinte é classificado como não infectado, seu status será alterado para *OK* somente se ele tiver sido verificado por três dias depois de ter sido movido para a Quarentena, ou depois disso.
- **Encerrar** – interrompe a execução do aplicativo.
- **Permitir** – permite a execução do aplicativo.
- **Adicionar às exclusões** – permite que o aplicativo execute essas ações a qualquer momento no futuro.

APLICATIVO MALICIOSO OU APLICATIVO LEGAL QUE PODE SER USADO POR INVASORES DETECTADO

Se o Antivírus de Arquivos, o Antivírus de Email ou a tarefa de verificação de vírus detectar um aplicativo suspeito ou um aplicativo legal que pode ser usado por invasores, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto. Clique nele para abrir a janela com informações sobre o objeto. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus, onde pode obter mais detalhes.
- Nome do arquivo do objeto, incluindo seu caminho.

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Quarentena** – move o objeto para a Quarentena, onde ele não representa uma ameaça ao computador. Esta opção estará disponível se a ameaça for desconhecida e nenhum dos métodos de desinfecção existentes puder ser aplicado ao objeto.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status de *não infectado* e ele pode ser restaurado.

  Se você mover manualmente para a Quarentena um arquivo que na verificação seguinte é classificado como não infectado, seu status será alterado para *OK* somente se ele tiver sido verificado por três dias depois de ter sido movido para a Quarentena, ou depois disso.

- **Excluir** – exclui o objeto. Antes da exclusão, é criada uma cópia de backup do objeto para que ele possa ser restaurado posteriormente ou para poder rastrear a forma de infecção.

- **Excluir arquivo comprimido** - exclui o arquivo comprimido protegido por senha.

- **Ignorar/Bloquear** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Você pode retornar ao processamento de objetos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.

- **Adicionar às exclusões** - cria uma regra de exclusão para este tipo de ameaça.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar para todos os objetos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o aplicativo ser reiniciado, ou o período entre o início e a conclusão de uma verificação de vírus.

Se tiver certeza de que o objeto detectado não é malicioso, é recomendável adicioná-lo à zona confiável para evitar que o programa gere falsos positivos quando você usar o objeto.

LINK SUSPEITO/MALICIOSO DETECTADO

Quando o Kaspersky Anti-Virus detecta uma tentativa de ir para um site com conteúdo suspeito ou malicioso, uma notificação especial é exibida na tela.

A notificação fornece as seguintes informações:

- descrição da ameaça;
- nome do aplicativo (navegador) usado pelo site;
- URL do site ou da página da Web com conteúdo suspeito ou malicioso.

Você pode selecionar uma das seguintes ações:

- **Permitir** – continua o download do site.
- **Bloquear** – bloqueia o download do site.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual do componente de proteção, marque a caixa **Aplicar para todos os objetos**. A sessão atual do aplicativo consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou reiniciado.

OBJETO PERIGOSO DETECTADO NO TRÁFEGO

Quando o Antivírus da Web detecta um objeto malicioso no tráfego, é exibida uma notificação pop-up especial na tela.

A notificação contém as seguintes informações:

- Descrição da ameaça ou das ações executadas pelo aplicativo.
- Nome do aplicativo que executa a ação.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto malicioso. Clique nele para abrir a janela com informações sobre o objeto. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.
- Local do objeto (URL).

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Permitir** – continua o download do objeto.
- **Bloquear** – bloqueia o download do objeto do recurso da Web.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar para todos os objetos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o aplicativo ser reiniciado, ou o período entre o início e a conclusão de uma verificação de vírus.

TENTATIVA DE ACESSO A UM SITE DE PHISHING DETECTADA

Quando o Kaspersky Anti-Virus detecta uma tentativa de acessar um site que é ou pode ser um site de phishing, uma notificação especial é exibida na tela.

A notificação fornece as seguintes informações:

- descrição da ameaça;
- URL do site.

É solicitado que você selecione uma das seguintes ações:

- **Permitir** – continua o download do site.
- **Bloquear** – bloqueia o download do site.

Para aplicar a ação selecionada a todos os sites com o mesmo status detectados na sessão atual do Kaspersky Anti-Virus, marque a caixa **Aplicar para todos os objetos**. A sessão atual do aplicativo consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou reiniciado.

TENTATIVA DE ACESSO AO REGISTRO DO SISTEMA DETECTADA

Quando a Defesa Proativa detecta uma tentativa de acessar as chaves do Registro do sistema, é exibida uma notificação pop-up.

A notificação fornece as seguintes informações:

- a chave do Registro que está sendo acessada;
- o nome do arquivo do processo que iniciou a tentativa de acesso às chaves do Registro, incluindo seu caminho.

É solicitado que você selecione uma das seguintes ações:

- **Permitir** – permite a execução da ação perigosa uma vez;
- **Bloquear** – bloqueia a ação perigosa uma vez.

Para executar automaticamente a ação selecionada sempre que essa atividade for iniciada no computador, marque a caixa **Criar uma regra**.

Se tiver certeza de que as atividades do aplicativo que tentou acessar as chaves do Registro do sistema não são perigosas, adicione o aplicativo à lista de aplicativos confiáveis.

O OBJETO NÃO PODE SER DESINFETADO

Em alguns casos, não é possível desinfetar um objeto malicioso; por exemplo, se o arquivo estiver tão danificado que o aplicativo não consegue remover o código malicioso e restaurar sua integridade. O procedimento de neutralização não pode ser aplicado a diversos tipos de objetos perigosos, como os cavalos de Troia. Nesse caso, uma notificação é exibida na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

O ícone é exibido ao lado do nome do objeto malicioso. Clique nele para abrir a janela com informações sobre o objeto. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.

- Nome do arquivo do objeto malicioso, incluindo seu caminho.

É solicitado que você selecione uma das seguintes respostas em relação ao objeto:

- **Excluir** – exclui o objeto. Antes da exclusão, é criada uma cópia de backup do objeto para que ele possa ser restaurado posteriormente ou para poder rastrear a forma de infecção.
- **Ignorar/Bloquear** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Você pode retornar ao processamento de objetos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.

Para aplicar a ação selecionada a todos os objetos com o mesmo status detectados na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar para todos os objetos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o aplicativo ser reiniciado, ou o período entre o início e a conclusão de uma verificação de vírus.

PROCESSO OCULTO DETECTADO

Se a Defesa Proativa detectar um processo oculto no sistema, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo e nome da ameaça conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome. Clique nele para abrir a janela com informações sobre a ameaça. Ao clicar no link www.securelist.com/en/ nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça.
- Nome do arquivo do processo, incluindo seu caminho.

É solicitado que você selecione uma das seguintes ações:

- **Quarentena** – fecha o processo e move o arquivo do processo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status de *não infectado* e ele pode ser restaurado.

  > Se você mover manualmente para a Quarentena um arquivo que na verificação seguinte é classificado como não infectado, seu status será alterado para *OK* somente se ele tiver sido verificado por três dias depois de ter sido movido para a Quarentena, ou depois disso.

- **Encerrar** – interrompe o processo.
- **Permitir** – permite a execução do processo.

Para aplicar a ação selecionada a todos os processos ocultos com o mesmo status detectados na sessão atual da Defesa Proativa, marque a caixa **Nesses casos, sempre executar**. A sessão atual do aplicativo consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou reiniciado.

Se tiver certeza de que o processo detectado não é perigoso, é recomendável adicioná-lo à zona confiável para evitar que o Kaspersky Anti-Virus repita falsos positivos ao detectá-lo.

TRABALHANDO COM O APLICATIVO NA LINHA DE COMANDO

Você pode trabalhar com o Kaspersky Anti-Virus usando a linha de comando. É possível executar as seguintes operações:

- ativar o aplicativo;
- iniciar e interromper o aplicativo;
- iniciar e interromper componentes do aplicativo;
- iniciar e interromper as tarefas;
- obter informações sobre o status atual dos componentes e das tarefas, além de suas estatísticas;
- iniciar e interromper tarefas de verificação de vírus;
- verificar os objetos selecionados;
- atualizar os bancos de dados e módulos do software, reverter atualizações;
- exportar e importar configurações de segurança;
- abrir os arquivos da ajuda usando a sintaxe geral da linha de comando e de comandos individuais.

Sintaxe do prompt de comando:

```
avp.com <comando> [opções]
```

Acesse o aplicativo na linha de comando a partir da pasta de instalação do aplicativo ou especificando o caminho completo de avp.com.

A lista de comandos usados para controlar o aplicativo e seus componentes é fornecida na tabela a seguir.

START	Inicia um componente ou uma tarefa.
STOP	Interrompe um componente ou uma tarefa. O comando poderá ser executado somente se a senha atribuída através da interface do Kaspersky Anti-Virus for inserida.
STATUS	Exibe o status atual do componente ou da tarefa na tela.
STATISTICS	Exibe estatísticas do componente ou da tarefa na tela.
HELP	Exibe a lista de comandos e informações sobre a sintaxe de comandos.
SCAN	Verificação de objetos quanto à presença de vírus.
UPDATE	Inicia a atualização do aplicativo.
ROLLBACK	Reverte para a última atualização do Kaspersky Anti-Virus. O comando poderá ser executado somente se a senha atribuída através da interface do aplicativo for inserida.
EXIT	Fecha o aplicativo. O comando poderá ser executado somente se a senha atribuída através da interface do aplicativo for inserida.

IMPORT	Importa as configurações de proteção do aplicativo. O comando poderá ser executado somente se a senha atribuída através da interface do Kaspersky Anti-Virus for inserida.
EXPORT	Exporta as configurações de proteção do aplicativo.

Cada comando exige seu próprio conjunto específico de configurações.

NESTA SEÇÃO:

Ativando o aplicativo 165

Iniciando o aplicativo 165

Interrompendo o aplicativo 166

Gerenciando componentes e tarefas do aplicativo 166

Verificação de vírus 167

Atualizando o aplicativo 170

Revertendo a última atualização 171

Exportando as configurações de proteção 171

Importando as configurações de proteção 171

Criando um arquivo de rastreamento 172

Exibindo a Ajuda 172

Códigos de retorno da linha de comando 172

ATIVANDO O APLICATIVO

É possível ativar o Kaspersky Anti-Virus usando um arquivo de chave.

Sintaxe do comando:

```
avp.com ADDKEY <nome_do_arquivo)>
```

A tabela a seguir descreve as configurações de desempenho do comando.

<nome_do_arquivo>	Nome do arquivo de chave do aplicativo com a extensão *.key

Exemplo:

```
avp.com ADDKEY 1AA111A1.key
```

INICIANDO O APLICATIVO

Sintaxe do comando:

```
avp.com
```

INTERROMPENDO O APLICATIVO

Sintaxe do comando:

```
avp.com EXIT /password=<sua_senha>
```

A descrição dos parâmetros é fornecida na tabela a seguir.

<sua_senha>	Senha do aplicativo especificada na interface

Este comando não será aceito sem uma senha.

GERENCIANDO COMPONENTES E TAREFAS DO APLICATIVO

Sintaxe do comando:

```
avp.com <comando> <perfil|nome_da_tarefa> [/R[A]:<arquivo_de_relatório>]
```

```
avp.com STOP <profile|nome_da_tarefa> /password=<sua_senha>
[/R[A]:<arquivo_de_relatório>]
```

A tabela a seguir fornece as descrições de comandos e configurações.

<comando>	Você pode gerenciar as tarefas e os componentes do Kaspersky Anti-Virus a partir do prompt de comando, com os seguintes comandos: START – inicia uma tarefa ou um componente de proteção. STOP – interrompe uma tarefa ou um componente de proteção. STATUS – exibe o status atual da tarefa ou do componente de proteção. STATISTICS – exibe na tela as estatísticas da tarefa ou do componente de proteção. O comando STOP não será aceito sem uma senha.
<perfil|nome_da_tarefa>	Você pode especificar qualquer componente de proteção, módulo dos componentes, tarefa de verificação por demanda ou de atualização do Kaspersky Anti-Virus como valor da configuração **<perfil>** (os valores padrão usados pelo aplicativo são mostrados na tabela a seguir). Você pode especificar o nome de qualquer tarefa de atualização ou verificação por demanda como valor da configuração **<nome_da_tarefa>**.
<sua_senha>	Senha do aplicativo especificada na interface.
/R[A]:<arquivo_de_relatório>	**/R:<arquivo_de_relatório>** – registra somente os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Na configuração **<perfil>**, especifique um dos valores fornecidos na tabela a seguir.

RTP	Todos os componentes de proteção. O comando **avp.com START RTP** executa todos os componentes de proteção, se a proteção tiver sido totalmente desativada. Se o componente tiver sido desativado usando o comando **STOP** no prompt de comando, ele não será iniciado pelo comando **avp.com START RTP**. Para iniciá-lo, execute o comando **avp.com START <perfil>** com o nome do componente de proteção específico inserido em **<perfil>**. Por exemplo, **avp.com START FM**.
pdm	Defesa Proativa.
FM	Antivírus de Arquivos.
EM	Antivírus de Email.
WM	Antivírus da Web. Valores dos subcomponentes do Antivírus da Web: **httpscan (HTTP)** – verifica o tráfego HTTP; **sc** – verifica scripts.
IM	Antivírus de IM.
Updater	Atualização.
Rollback	Reversão da última atualização.
Scan_My_Computer	Verificação.
Scan_Objects	Verificação Personalizada.
Scan_Quarantine	Verificação da Quarentena.
Scan_Startup (STARTUP)	Verificação de Objetos de Inicialização.
Scan_Vulnerabilities (SECURITY)	Verificação de Vulnerabilidades.

Os componentes e tarefas iniciados no prompt de comando são executados com as configurações definidas na interface do aplicativo.

Exemplos:

- *Para ativar o Antivírus de Arquivos:*

```
avp.com START FM
```

- *Para interromper a verificação do computador:*

```
avp.com STOP Scan_My_Computer /password=<sua_senha>
```

VERIFICAÇÃO DE VÍRUS

Para iniciar uma verificação de vírus em uma determinada área e processar objetos maliciosos no prompt de comando:

```
avp.com SCAN [<objeto verificado>] [<ação>] [<tipos de arquivos>] [<exclusões>]
[<arquivo de configuração>] [<configurações relatório>] [<configurações avançadas>]
```

Para verificar objetos, você também pode usar as tarefas criadas no aplicativo, iniciando-as na linha de comando. A tarefa será executada com as configurações especificadas na interface do Kaspersky Anti-Virus.

A descrição dos parâmetros é fornecida na tabela a seguir.

<objeto a ser verificado> – este parâmetro fornece a lista de objetos que serão verificados quanto à presença de código malicioso. Ele pode incluir vários valores da lista fornecida separados por espaços.	
<arquivos>	Lista dos caminhos de arquivos e pastas que devem ser verificados. Você pode inserir um caminho absoluto ou relativo para o arquivo. Os itens da lista são separados por um espaço. Comentários: • Se o nome do objeto contiver um espaço, será necessário colocá-lo entre aspas. • Se for feita uma referência a uma pasta específica, todos os arquivos da pasta serão verificados.
/MEMORY	Objetos da RAM.
/STARTUP	Objetos de inicialização.
/MAIL	Caixas de correio.
/REMDRIVES	Todas as unidades de mídia removíveis.
/FIXDRIVES	Todas as unidades internas.
/NETDRIVES	Todas as unidades de rede.
/QUARANTINE	Objetos da Quarentena.
/@:<filelist.lst>	Caminho para um arquivo que contém uma lista de objetos e catálogos a serem verificados. Você pode inserir um caminho absoluto ou relativo para o arquivo com a lista. Mesmo que contenha espaços, o caminho deverá ser colocado sem aspas. O arquivo com a lista de objetos deve estar em formato de texto. Cada objeto de verificação deve estar listado em uma linha separada. É recomendável especificar caminhos absolutos para os objetos de verificação no arquivo. Ao especificar um caminho relativo, ele é especificado em relação ao arquivo executável de um aplicativo e não em relação ao arquivo com a lista de objetos de verificação.
<ação> – este parâmetro determina que ações serão executadas com objetos maliciosos detectados durante a verificação. Se o parâmetro não for definido, a ação padrão será aquela com o valor **/i8**. Se estiver trabalhando no modo automático, o Kaspersky Anti-Virus aplicará automaticamente a ação recomendada pelos especialistas da Kaspersky Lab ao detectar objetos perigosos. Uma ação que corresponda ao valor do parâmetro **<ação>** será ignorada.	
/i0	Não é tomada nenhuma ação em relação ao objeto; suas informações são registradas no relatório.
/i1	Neutraliza objetos infectados e, se a desinfecção falhar, os ignora.
/i2	Neutraliza objetos infectados e, se a desinfecção falhar, os exclui. Não exclui objetos infectados de objetos compostos. Exclui objetos compostos infectados com cabeçalhos executáveis (arquivos comprimidos sfx) (esta é a configuração padrão).
/i3	Neutraliza objetos infectados e, se a desinfecção falhar, os exclui. Exclui completamente todos os objetos compostos, se não for possível excluir as partes infectadas.

/i4	Exclui os objetos infectados. Exclui completamente todos os objetos compostos, se não for possível excluir as partes infectadas.
/i8	Pergunta o que fazer se for detectado um objeto infectado.
/i9	Pergunta o que fazer no final da verificação.
<tipos_de_arquivos> – este parâmetro define os tipos de arquivos que estarão sujeitos à verificação antivírus. Por padrão, se esse parâmetro não for definido, apenas os arquivos infectados por conteúdo serão verificados.	
/fe	Verifica somente os arquivos que podem ser infectados de acordo com sua extensão.
/fi	Verifica somente os arquivos que podem ser infectados de acordo com seu conteúdo.
/fa	Verifica todos os arquivos.
<exclusões> – este parâmetro define os objetos excluídos da verificação. Ele pode incluir vários valores da lista fornecida separados por espaços.	
-e:a	Não verifica arquivos comprimidos.
-e:b	Não verifica bancos de dados de email.
-e:m	Não verifica emails em texto sem formatação.
-e:<máscara_arquivos>	Não verifica objetos que correspondem à máscara.
-e:<segundos>	Ignora objetos cujo tempo de verificação ultrapassa o tempo especificado no parâmetro **<segundos>**.
-es:<tamanho>	Ignora objetos cujo tamanho (em MB) excede o valor especificado na configuração **<tamanho>**. Esta configuração estará disponível apenas para arquivos compostos (como arquivos comprimidos).
<arquivo de configuração> – define o caminho do arquivo de configuração que contém as configurações de verificação do aplicativo. O arquivo de configuração está no formato de texto e contém o conjunto de parâmetros da linha de comando para a verificação antivírus. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores definidos na interface do aplicativo.	
/C:<nome_do_arquivo>	Usa os valores das configurações especificadas no arquivo **<nome_do_arquivo>**.
<configurações relatório> – este parâmetro determina o formato do relatório de resultados da verificação. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.	
/R:<arquivo_de_relatório>	Registra apenas os eventos importantes nesse arquivo.
/RA:<arquivo_de_relatório>	Registra todos os eventos nesse arquivo.

<configurações avançadas> – configurações que definem o uso das tecnologias de verificação antivírus.	
/iChecker=<on|off>	Ativa/desativa o uso da tecnologia iChecker.
/iSwift=<on|off>	Ativa/desativa o uso da tecnologia iSwift.

Exemplos:

- *Iniciar a verificação da memória, dos programas de inicialização, das caixas de correio, dos diretórios Meus documentos e Arquivos de programas e do arquivo test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\Meus documentos" "C:\Arquivos de programas" "C:\Downloads\test.exe"
```

- *Verificar os objetos listados no arquivo object2scan.txt. Usar o arquivo de configuração scan_settings.txt. Ao concluir a verificação, criar um relatório de todos os eventos:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Um exemplo de arquivo de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

ATUALIZANDO O APLICATIVO

A sintaxe para atualizar os módulos do Kaspersky Anti-Virus e os bancos de dados do aplicativo da linha de comando é a seguinte:

```
avp.com UPDATE [<fonte_de_atualização>] [/R[A]:<arquivo_de_relatório>] [/C:<nome_do_arquivo>]
```

A descrição dos parâmetros é fornecida na tabela a seguir.

<fonte_de_atualização>	Servidor HTTP ou FTP ou pasta de rede para baixar as atualizações. O valor do parâmetro pode estar no formato de um caminho completo para uma fonte de atualização ou um URL. Se não for selecionado um caminho, a fonte da atualização será obtida da configurações de atualização do aplicativo.
/R[A]:<arquivo_de_relatório>	**/R:<arquivo_de_relatório>** – registra somente os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
/C:<nome_do_arquivo>	Caminho do arquivo de configuração da atualização do Kaspersky Anti-Virus. O arquivo de configuração está no formato de texto sem formatação e contém uma lista de parâmetros da linha de comando para a atualização do aplicativo. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se esse parâmetro não for definido, serão usados os valores definidos na interface do aplicativo.

Exemplos:

- *Atualizar os bancos de dados do aplicativo e registrar todos os eventos no relatório:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Atualizar os módulos do Kaspersky Anti-Virus usando as configurações do arquivo de configuração updateapp.ini:*

```
avp.com UPDATE /C:updateapp.ini
```

Um exemplo de arquivo de configuração:

```
"ftp://meu_servidor/kav updates" /RA:avbases_upd.txts
```

REVERTENDO A ÚLTIMA ATUALIZAÇÃO

Sintaxe do comando:

```
avp.com ROLLBACK [/R[A]:<arquivo_de_relatório>][/password=<sua_senha>]
```

A descrição dos parâmetros é fornecida na tabela a seguir.

/R[A]:<arquivo_de_relatório>	**/R:<arquivo_de_relatório>** – registra somente os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
<sua_senha>	Senha do aplicativo especificada na interface.

Este comando não será aceito sem uma senha.

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt /password=<sua_senha>
```

EXPORTANDO AS CONFIGURAÇÕES DE PROTEÇÃO

Sintaxe do comando:

```
avp.com EXPORT <perfil> <nome_do_arquivo>
```

A tabela a seguir descreve as configurações de desempenho do comando.

<perfil>	Componente ou tarefa cujas configurações estão sendo exportadas. Para a configuração **<perfil>**, você pode usar qualquer valor listado na seção da Ajuda "Gerenciando componentes e tarefas do aplicativo".
<nome_do_arquivo>	Caminho do arquivo para o qual as configurações do Kaspersky Anti-Virus são exportadas. É possível especificar um caminho absoluto ou relativo. Se nenhum formato for especificado, o arquivo de configuração será salvo no formato binário (DAT) e poderá ser usado posteriormente para exportar as configurações do aplicativo para outros computadores. O arquivo de configuração também pode ser gravado como um arquivo de texto. Para fazê-lo, digite a extensão *.txt* no nome do arquivo. Não é possível importar configurações de proteção de um arquivo de texto. Este arquivo pode ser usado somente para especificar as principais configurações de operação do Kaspersky Anti-Virus.

Exemplo:

```
avp.com EXPORT RTP c:\settings.dat
```

IMPORTANDO AS CONFIGURAÇÕES DE PROTEÇÃO

Sintaxe do comando:

```
avp.com IMPORT <nome_do_arquivo> [/password=<sua_senha>]
```

A tabela a seguir descreve as configurações de desempenho do comando.

<nome_do_arquivo>	Caminho do arquivo do qual as configurações do Kaspersky Anti-Virus são importadas. É possível especificar um caminho absoluto ou relativo.
<sua_senha>	Senha do Kaspersky Anti-Virus especificada na interface do aplicativo. Os parâmetros de segurança podem ser importados somente de um arquivo binário.

Este comando não será aceito sem uma senha.

Exemplo:

```
avp.com IMPORT c:\ settings.dat /password=<sua_senha>
```

CRIANDO UM ARQUIVO DE RASTREAMENTO

A criação de um arquivo de rastreamento pode ser necessária no caso de problemas na operação do Kaspersky Anti-Virus. Isso ajudará os especialistas de Suporte Técnico a diagnosticar os problemas com mais precisão.

É recomendável criar arquivos de rastreamento apenas para a solução de um problema específico. A ativação normal do rastreamento pode tornar o computador lento e sobrecarregar o disco rígido.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off] [<nível_de_rastreamento>]
```

A descrição dos parâmetros é fornecida na tabela a seguir.

[on|off]	Ativa/desativa a criação do arquivo de rastreamento.
[file]	Saída do rastreamento em arquivo.
<nível_de_rastreamento>	Este valor pode ser um valor de 0 (nível mínimo, apenas mensagens críticas) a 700 (nível máximo, todas as mensagens). O Suporte Técnico o informará sobre o nível de rastreamento necessário quando você entrar em contato. Se o nível não for especificado, é recomendável configurá-lo como 500.

Exemplos:

- *Para desativar a criação do arquivo de rastreamento:*

```
avp.com TRACE file off
```

- *Para criar um arquivo de rastreamento para enviar ao Suporte Técnico com um nível de rastreamento máximo de 500:*

```
avp.com TRACE file on 500
```

EXIBINDO A AJUDA

O comando a seguir é usado para exibir a ajuda da sintaxe da linha de comando:

```
avp.com [ /? | HELP ]
```

Você pode usar um dos seguintes comandos para exibir informações de ajuda da sintaxe de um comando específico:

```
avp.com <comando> /?
avp.com HELP <comando>
```

CÓDIGOS DE RETORNO DA LINHA DE COMANDO

Esta seção descreve os códigos de retorno da linha de comando (veja a tabela a seguir). Os códigos gerais podem ser retornados por qualquer comando da linha de comando. Os códigos de retorno incluem códigos gerais e códigos específicos de um determinado tipo de tarefa.

CÓDIGOS DE RETORNO GERAIS	
0	Operação concluída com êxito
1	Valor de configuração inválido
2	Erro desconhecido
3	Erro ao concluir a tarefa
4	Tarefa cancelada
CÓDIGOS DE RETORNO DA TAREFA DE VERIFICAÇÃO DE VÍRUS	
101	Todos os objetos perigosos foram processados
102	Objetos perigosos detectados

GLOSSÁRIO

A

ANALISADOR HEURÍSTICO

Tecnologia de detecção de ameaças que não podem ser detectadas usando os bancos de dados de antivírus. Permite detectar objetos suspeitos de infecção por um vírus desconhecido ou por uma nova modificação de vírus conhecidos.

O analisador heurístico detecta até 92% das ameaças. Esse mecanismo é bastante eficiente e raramente produz falsos positivos.

Os arquivos detectados pelo analisador heurístico são considerados suspeitos.

APLICATIVO INCOMPATÍVEL

Aplicativo antivírus de outro desenvolvedor ou aplicativo da Kaspersky Lab que não dá suporte ao gerenciamento por meio do Kaspersky Internet Security.

ARQUIVO COMPACTADO

Um arquivo comprimido que contém um programa de descompactação e instruções para sua execução pelo sistema operacional.

ARQUIVO COMPRIMIDO

Arquivo que "contêm" um ou vários outros objetos que também podem ser arquivos comprimidos.

ARQUIVO DE CHAVE

Arquivo com a extensão .key que é sua "chave" pessoal, necessária para a operação do aplicativo da Kaspersky Lab. Um arquivo de chave é fornecido com o produto, se você o comprar dos distribuidores da Kaspersky Lab, ou enviado por email, se você comprar o produto online.

ATIVANDO O APLICATIVO

Alterna o aplicativo para o modo totalmente funcional. O usuário precisa de uma licença para ativar o aplicativo.

ATUALIZAÇÃO

Procedimento de substituição/adição de novos arquivos (bancos de dados ou módulos do aplicativo) recuperados dos servidores de atualização da Kaspersky Lab.

ATUALIZAÇÃO DOS BANCOS DE DADOS

Uma das funções executadas pelos aplicativos da Kaspersky Lab que permitem manter a proteção atualizada. Ao fazê-lo, os bancos de dados são baixados dos servidores de atualização da Kaspersky Lab para o computador e são conectados automaticamente ao aplicativo.

ATUALIZAÇÕES DISPONÍVEIS

Um conjunto de atualizações dos módulos do aplicativo da Kaspersky Lab que inclui as atualizações críticas acumuladas por um determinado período e as alterações da arquitetura do aplicativo.

ATUALIZAÇÕES URGENTES

Atualizações críticas dos módulos do aplicativo da Kaspersky Lab.

B

BANCO DE DADOS DE ENDEREÇOS DA WEB SUSPEITOS

Lista de endereços da Web cujo conteúdo pode ser considerado como possivelmente perigoso. Essa lista é criada pelos especialistas da Kaspersky Lab. Ela é atualizada periodicamente, sendo incluída no pacote do aplicativo da Kaspersky Lab.

BANCO DE DADOS DE ENDEREÇOS DE PHISHING

Lista de endereços da Web definidos pelos especialistas da Kaspersky Lab como endereços de phishing. O banco de dados é atualizado periodicamente e faz parte do aplicativo da Kaspersky Lab.

BANCOS DE DADOS

Bancos de dados criados pelos especialistas da Kaspersky Lab, que contêm descrições detalhadas de todas as ameaças atuais à segurança do computador, além dos métodos usados para sua detecção e desinfecção. Esses bancos de dados são atualizados pela Kaspersky Lab constantemente conforme surgem novas ameaças. Para obter uma detecção de ameaças de alta qualidade, é recomendável copiar os bancos de dados dos servidores de atualização da Kaspersky Lab periodicamente.

BANCOS DE DADOS DE EMAIL

Bancos de dados que contêm emails em um formato especial e que são salvos no computador. Cada email enviado/recebido é colocado no banco de dados de email depois de ser enviado/recebido. Esses bancos de dados são verificados durante a verificação completa do computador.

Os emails são analisados em tempo real quanto à presença de vírus no momento em que são enviados e recebidos, se a proteção em tempo real estiver ativada.

BLOQUEIO DO OBJETO

Negação de acesso de aplicativos externos a um objeto. Um objeto bloqueado não pode ser lido, executado, alterado ou excluído.

C

CABEÇALHO

Informações no início de um arquivo ou uma mensagem que compreendem dados de nível inferior sobre o processamento e o status do arquivo (ou mensagem). Particularmente, o cabeçalho de emails contém dados como informações sobre o remetente e o destinatário, além da data.

CERTIFICADO DO SERVIDOR DE ADMINISTRAÇÃO

O certificado que permite a autenticação do Servidor de administração ao conectar o Console de administração a ele e ao trocar dados com os computadores dos usuários. O certificado do Servidor de administração é criado na instalação do Servidor de administração e é armazenado na subpasta Cert da pasta de instalação do aplicativo.

CLASSIFICAÇÃO DE AMEAÇA

Classificação do nível de perigo que um aplicativo representa para o sistema operacional. A classificação é calculada usando a análise heurística com base em dois tipos de critérios:

estáticos (como as informações sobre o arquivo executável de um aplicativo: tamanho, data de criação, etc.);

dinâmicos, que são usados ao simular a operação do aplicativo em um ambiente virtual (análise das chamadas de funções do sistema pelo aplicativo).

A classificação de ameaça permite detectar um comportamento típico de malware. Quando menor for a classificação de ameaça, o aplicativo terá permissão de executar mais ações no sistema.

CONFIGURAÇÕES DA TAREFA

Configurações do aplicativo que são específicas de cada tipo de tarefa.

CONFIGURAÇÕES DO APLICATIVO

Configurações do aplicativo que são comuns a todos os tipos de tarefa, regulando a operação do aplicativo como um todo, como as configurações de desempenho do aplicativo, as configurações de relatórios e as configurações de armazenamento no backup.

CONTADOR DE SURTO DE VÍRUS

Modelo baseado no qual é gerada a notificação sobre surtos de vírus. O contador de surto de vírus inclui uma combinação de configurações que determinam o limite da atividade de vírus, sua forma de disseminação e texto das mensagens que devem ser enviadas.

D

DESINFECÇÃO DE OBJETOS

Método usado para processar objetos infectados que resulta na recuperação completa ou parcial dos dados, ou na decisão de que os objetos não podem ser desinfetados. Os objetos são desinfetados usando os registros do banco de dados. Parte dos dados pode ser perdida durante a desinfecção.

DESINFECÇÃO DE OBJETOS AO REINICIAR

Método de processamento de objetos infectados que estão sendo usados por outros aplicativos no momento da desinfecção. Consiste em criar uma cópia do objeto infectado, desinfetar a cópia criada e substituir o objeto original infectado pela cópia desinfetada na próxima reinicialização do sistema.

DNS (SERVIÇO DE NOMES DE DOMÍNIO)

Sistema distribuído para converter o nome de um host (um computador ou outro dispositivo de rede) em endereço IP. O DNS funciona em redes TCP/IP. O DNS também pode armazenar e processar solicitações reversas, determinando o nome de um host por seu endereço (registro PTR). Normalmente, a resolução de nomes DNS é executada pelos aplicativos de rede, não pelos usuários.

E

EXCLUSÃO

A exclusão é um objeto excluído da verificação pelo aplicativo da Kaspersky Lab. Você pode excluir da verificação arquivos de determinados formatos, máscaras de arquivos, uma determinada área (por exemplo, uma pasta ou um programa), processos de aplicativos ou objetos por tipo de ameaça, de acordo com a classificação da Enciclopédia de Vírus. A cada tarefa pode ser atribuído um conjunto de exclusões.

EXCLUSÃO DE MENSAGENS

Método de processamento de um email que contém sinais de spam, no qual a mensagem é removida fisicamente. É recomendável aplicar esse método às mensagens que com certeza contêm spam. Antes de excluir uma mensagem, uma cópia da mesma é salva no backup (a menos que essa opção esteja desativada).

EXCLUSÃO DE UM OBJETO

Método de processamento de objetos que os exclui fisicamente de seu local original (disco rígido, pasta, recurso de rede). É recomendável aplicar esse método a objetos perigosos que, por algum motivo, não podem ser desinfetados.

F

FALSO POSITIVO

Situação em que o aplicativo da Kaspersky Lab considera um objeto não infectado como infectado devido à semelhança de seu código com o de um vírus.

FLUXOS NTFS ALTERNATIVOS

Fluxos de dados NTFS (fluxos de dados alternativos) criados para conter informações de arquivos ou atributos adicionais.

Cada arquivo do sistema de arquivos NTFS é um conjunto de fluxos. Um deles armazena o conteúdo do arquivo que poderá ser exibido ao abrir o arquivo; os outros fluxos (os chamados alternativos) foram criados para conter metainformações e assegurar, por exemplo, a compatibilidade do NTFS com outros sistemas, como um sistema de arquivos mais antigo da Macintosh chamado HFS (Hierarchical File System). Os fluxos podem ser criados, excluídos, armazenados separadamente, renomeados e até mesmo executados como um processo.

Os fluxos alternativos podem ser usados por invasores para transferir dados ocultamente ou para roubá-los de um computador.

G

GATEWAY DUPLO

Computador equipado com dois adaptadores de rede (cada um conectado a redes diferentes) que transferem dados de uma rede para outra.

H

HOOK

Subcomponente do aplicativo responsável pela verificação de tipos específicos de email. O conjunto de interceptadores específicos à sua instalação depende da função e da combinação de funções para as quais o aplicativo está sendo implantado.

I

INSTALAÇÃO COM UM CENÁRIO DE INICIALIZAÇÃO

Método de instalação remota dos aplicativos da Kaspersky Lab que permite atribuir a inicialização da tarefa de instalação remota a uma conta de usuário individual (ou a várias contas de usuário). O registro de um usuário em um domínio leva a uma tentativa de instalar o aplicativo no computador cliente no qual o usuário foi registrado. Esse método é recomendável para a instalação dos aplicativos em computadores que executam sistemas operacionais Microsoft Windows 98/ME.

IP (PROTOCOLO IP)

O protocolo básico da Internet, usado sem alterações desde seu desenvolvimento, em 1974. Executa as operações básicas de transmissão de dados de um computador para outro e serve como base para protocolos de nível superior, como o TCP e o UDP. Gerencia a conexão e o processamento de erros. Tecnologias como a NAT e as máscaras possibilitam ocultar muitas redes particulares usando um pequeno número de endereços IP (ou até mesmo um endereço). Assim, é possível atender à demanda cada vez maior de crescimento da Internet usando o espaço relativamente restrito de endereços IPv4.

K

KASPERSKY SECURITY NETWORK

O Kaspersky Security Network (KSN) é uma infraestrutura de serviços online que dá acesso à Base de Dados de Conhecimento online da Kaspersky Lab, que contém informações sobre a reputação de arquivos, recursos da Web e software. A utilização de dados do Kaspersky Security Network garante um tempo de resposta menor do Kaspersky Internet Security ao encontrar novos tipos de ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

L

LICENÇA ADICIONAL

Uma licença que foi adicionada para a operação do aplicativo da Kaspersky Lab, mas que ainda não foi ativada. A licença adicional entra em vigor quando a licença ativa expira.

LICENÇA ATIVA

A licença usada no momento para a operação de um aplicativo da Kaspersky Lab. A licença define a data de expiração da funcionalidade completa e a diretiva de licenças do aplicativo. O aplicativo não pode ter mais de uma licença com o status ativo.

LIMITE DE ATIVIDADE DE VÍRUS

O nível máximo permitido de um tipo de evento específico durante um período definido que, quando excedido, será considerado como atividade excessiva de vírus e ameaça de um surto de vírus. Esse recurso é importante durante os surtos de vírus e permite que um administrador reaja de forma oportuna às ameaças de surtos de vírus emergentes.

LISTA DE ENDEREÇOS DA WEB VERIFICADOS

Lista de máscaras e endereços de recursos da Web que são obrigatoriamente verificados quanto à presença de objetos maliciosos pelo aplicativo da Kaspersky Lab.

LISTA DE REMETENTES BLOQUEADOS

(também conhecida como lista "negra" de endereços)

A lista de endereços de email cujas mensagens devem ser bloqueadas pelo aplicativo da Kaspersky Lab, independentemente de seu conteúdo.

LISTA DE REMETENTES PERMITIDOS

(também conhecida como lista "branca" de endereços)

Lista de endereços de email cujas mensagens não devem ser verificadas pelo aplicativo da Kaspersky Lab.

LISTA DE URLS BLOQUEADOS

Lista de máscaras e endereços de recursos da Web cujo acesso é bloqueado pelo aplicativo da Kaspersky Lab. A lista de endereços é criada pelo usuário durante a configuração do aplicativo.

LISTA DE URLS CONFIÁVEIS

Lista de máscaras e endereços de recursos da Web em cujo conteúdo o usuário confia. O aplicativo da Kaspersky Lab não verifica as páginas da Web que correspondem aos itens da lista quanto à presença de objetos maliciosos.

LISTA DE URLS PERMITIDOS

Lista de máscaras e endereços de recursos da Web cujo acesso não é bloqueado pelo aplicativo da Kaspersky Lab. A lista de endereços é criada pelo usuário durante a configuração do aplicativo.

LISTA NEGRA DE ARQUIVOS DE CHAVE

Um banco de dados que contém informações sobre arquivos de chave da Kaspersky Lab contidos na lista negra. O conteúdo do arquivo da lista negra é atualizado juntamente com os bancos de dados do produto.

M

MÁSCARA DE ARQUIVOS

Representação de um nome de arquivo e extensão usando curingas. Os dois curingas padrão usados em máscaras de arquivos são * e ?, onde * representa qualquer número de caracteres e ? representa qualquer caractere. Com esses curingas, você pode representar qualquer arquivo. O nome e a extensão do arquivo sempre são separados por um ponto.

MÁSCARA DE SUB-REDE

A máscara de sub-rede (também conhecida como máscara de rede) e o endereço de rede determinam os endereços dos computadores em uma rede.

MENSAGEM OBSCENA

Email que contém linguagem ofensiva.

MENSAGEM SUSPEITA

Mensagem que não pode ser considerada spam com certeza, mas que parece suspeita à verificação (por exemplo, determinados tipos de correspondência e mensagens publicitárias).

MODELO DE NOTIFICAÇÃO

Modelo baseado no qual é gerada a notificação sobre objetos infectados detectados pela verificação. O modelo de notificação inclui uma combinação de configurações que regulam o modo de notificação, a forma de envio e o texto das mensagens que devem ser enviadas.

MÓDULOS DO APLICATIVO

Arquivos fornecidos no pacote de instalação da Kaspersky Lab responsáveis pela execução de suas principais tarefas. Um módulo executável específico corresponde a cada tipo de tarefa executada pelo aplicativo (proteção em tempo real, verificação por demanda, atualizações). Ao executar uma verificação completa do computador na janela principal, você inicia a execução do módulo dessa tarefa.

MOVIMENTAÇÃO DE OBJETOS PARA A QUARENTENA

Método de processamento de um objeto possivelmente infectado através do bloqueio do acesso ao arquivo e sua movimentação do seu local original para a pasta Quarentena, na qual o objeto é salvo em formato criptografado, o que elimina a ameaça de infecção.

N

NÍVEL DE GRAVIDADE DO EVENTO

Descrição do evento registrada durante a operação do aplicativo da Kaspersky Lab. Existem quatro níveis de gravidade:

Evento crítico.

Falha funcional.

Aviso.

Mensagem informativa.

Eventos do mesmo tipo podem ter diferentes níveis de gravidade, dependendo da situação em que o evento ocorreu.

NÍVEL DE SEGURANÇA

O nível de segurança é definido como uma configuração predefinida do componente.

NÍVEL RECOMENDADO

Nível de segurança baseado nas configurações do aplicativo recomendadas pelos especialistas da Kaspersky Lab a fim de fornecer o nível ideal de proteção do computador. Esse nível é definido para ser usado por padrão.

O

OBJETO INFECTADO

Objeto que contém um código malicioso. É detectado quando uma seção do código do objeto corresponde integralmente a uma seção do código de uma ameaça conhecida. A Kaspersky Lab não recomenda usar esses objetos, pois eles podem infectar o computador.

OBJETO INFECTÁVEL

Um objeto que, devido à sua estrutura ou ao seu formato, pode ser usado por invasores como um "contêiner" para armazenar e distribuir um objeto malicioso. Normalmente, são arquivos executáveis, por exemplo, arquivos com as extensões .com, .exe, .dll, etc. O risco de ativar códigos maliciosos nesses arquivos é bastante alto.

OBJETO MONITORADO

Um arquivo transferido pelos protocolos HTTP, FTP ou SMTP através do firewall e enviado para a verificação por um aplicativo da Kaspersky Lab.

OBJETO OLE

Um objeto anexado ou incorporado a outro arquivo. O aplicativo da Kaspersky Lab permite verificar vírus em objetos OLE. Por exemplo, se você inserir uma tabela do Microsoft Office Excel em um documento do Microsoft Office Word, a tabela será verificada como um objeto OLE.

OBJETO PERIGOSO

Objeto que contém um vírus. É recomendável não acessar esses objetos, pois isso poderia causar a infecção do seu computador. Quando um objeto infectado é detectado, é recomendável desinfetá-lo usando um dos aplicativos da Kaspersky Lab ou, caso a desinfecção não seja possível, excluí-lo.

OBJETO POSSIVELMENTE INFECTADO

Um objeto que contém o código de um vírus conhecido modificado ou um código que parece o código de um vírus, mas que ainda não é conhecido pela Kaspersky Lab. Arquivos possivelmente infectados são detectados usando o analisador heurístico.

OBJETO SUSPEITO

Um objeto que contém o código de um vírus conhecido modificado ou um código que parece o código de um vírus, mas que ainda não é conhecido pela Kaspersky Lab. Os objetos suspeitos são detectados usando o analisador heurístico.

OBJETOS DE INICIALIZAÇÃO

Conjunto de programas necessários para iniciar e operar corretamente o sistema operacional e os softwares instalados no computador. Esses objetos são executados sempre que o sistema operacional é iniciado. Existem vírus capazes de infectar esses objetos de forma específica e que podem levar, por exemplo, ao bloqueio do acesso ao sistema operacional.

P

PACOTE DE ATUALIZAÇÃO

Pacote de arquivos para a atualização do software. É baixado da Internet e instalado no computador.

PERÍODO DE VALIDADE DA LICENÇA

Período durante o qual você pode usar todos os recursos de seu aplicativo da Kaspersky Lab. Em geral, o período de validade da licença é de um ano a partir da data de instalação. Após a expiração da licença, a funcionalidade do aplicativo é reduzida. Você não poderá atualizar os bancos de dados do aplicativo.

PHISHING

Tipo de fraude da Internet que consiste no envio de emails com o objetivo de roubar informações confidenciais; normalmente, dados financeiros diversos.

PORTA DE ENTRADA/SAÍDA

Atende processadores (como os da Intel) para a troca de dados com componentes de hardware. A porta de entrada/saída está associada a um determinado componente de hardware e permite seu endereçamento por aplicativos para a troca de dados.

PORTA DE HARDWARE

Soquete em um componente de hardware de um computador no qual é possível conectar um cabo ou plugue (porta LPT, porta serial, porta USB).

PORTA DE REDE

Parâmetro TCP e UDP que determina o destino dos pacotes de dados no formato IP que são transmitidos para um host pela rede e possibilita que vários programas em execução em um único host recebam dados de forma independente. Cada programa processa os dados recebidos por uma determinada porta (às vezes se faz referência a isso dizendo que o programa "escuta" àquela porta).

Para alguns protocolos de rede comuns, geralmente existem números de porta padrão (por exemplo, geralmente os servidores Web recebem solicitações HTTP na porta TCP 80); no entanto, em geral, um programa pode usar qualquer protocolo em qualquer porta. Os valores possíveis são: 1 a 65535.

PROCESSO CONFIÁVEL

Processo de aplicativo cujas operações com arquivos não são monitoradas pelo aplicativo da Kaspersky Lab no modo de proteção em tempo real. Em outras palavras, os objetos executados, abertos ou salvos pelos processos confiáveis não serão verificados.

PROTEÇÃO EM TEMPO REAL

Modo de operação do aplicativo no qual os objetos são verificados em tempo real quanto à presença de código maliciosos.

O aplicativo intercepta todas as tentativas de abrir qualquer objeto (leitura, gravação ou execução) e verifica o objeto quanto à presença de ameaças. Os objetos não infectados são disponibilizados para o usuário; os objetos que contêm ameaças ou que são suspeitos de contê-las são processados de acordo com as configurações da tarefa (são desinfetados, excluídos ou colocados na Quarentena).

PROTOCOLO

Conjunto de regras claramente definido e padronizado que define a interação entre um cliente e um servidor. Protocolos conhecidos e os serviços associados a eles incluem o HTTP (WWW), o FTP e o NNTP (notícias).

Q

QUARENTENA

Uma pasta específica na qual são colocados todos os objetos possivelmente infectados detectados durante as verificações ou pela proteção em tempo real.

R

RESTAURAÇÃO

Movimentação de um objeto original da Quarentena ou do backup para a pasta na qual ele se encontrava originalmente, antes de ser movido para a Quarentena, desinfetado ou excluído, ou para uma outra pasta especificada pelo usuário.

S

SCRIPT

Um pequeno programa de computador ou uma parte independente de um programa (função) que, como regra, foi desenvolvida para executar uma pequena tarefa específica. É usado com mais frequência com programas incorporados no hipertexto. Os scripts são executados, por exemplo, quando você abre um determinado site.

Se a proteção em tempo real estiver ativada, o aplicativo controlará a execução dos scripts, os interceptará e verificará a presença de vírus. Dependendo dos resultados da verificação, você poderá bloquear ou permitir a execução do script.

SERVIDOR PROXY

Serviço de rede de computadores que permite aos usuários fazer solicitações indiretas a outros serviços de rede. Primeiro, um usuário se conecta a um servidor proxy e solicita um recurso (por exemplo, um arquivo) localizado em outro servidor. Em seguida, o servidor proxy se conecta ao servidor específico e obtém o recurso ou retorna o recurso de seu próprio cache (no caso de o proxy ter seu próprio cache). Em alguns casos, uma solicitação do usuário ou uma resposta do servidor pode ser modificada pelo servidor proxy.

SERVIDORES DE ATUALIZAÇÃO DA KASPERSKY LAB

Uma lista de servidores HTTP e FTP da Kaspersky Lab a partir dos quais o aplicativo baixa atualizações dos bancos de dados e módulos do aplicativo para o seu computador.

SETOR DE INICIALIZAÇÃO DO DISCO

O setor de inicialização é uma área específica no disco rígido, disquete ou outro dispositivo de armazenamento de dados do computador. Ele contém informações sobre o sistema de arquivos do disco e um programa de carregamento de inicialização responsável por iniciar o sistema operacional.

Existem diversos vírus que infectam os setores de inicialização, os chamados vírus de inicialização. O aplicativo da Kaspersky Lab permite verificar os setores de inicialização quanto à presença de vírus e desinfetá-los, caso seja detectada uma infecção.

SOCKS

Protocolo de servidor proxy que permite estabelecer uma conexão ponto-a-ponto entre computadores em redes internas e externas.

SPAM

Mensagens de email não solicitadas enviadas em massa, frequentemente contendo mensagens publicitárias.

STATUS DA PROTEÇÃO

O status atual da proteção que resume o nível de segurança do computador.

SURTO DE VÍRUS

Uma série de tentativas deliberadas de infectar um computador com vírus.

T

TAREFA

As funções executadas pelo aplicativo da Kaspersky Lab são implementadas como tarefas, como: Proteção em tempo real, Verificação completa do computador, Atualização do banco de dados.

TECNOLOGIA ICHECKER

O iChecker é uma tecnologia que aumenta a velocidade das verificações antivírus por meio da exclusão de objetos que permaneceram inalterados desde a última verificação, desde que os parâmetros de verificação (as configurações e o banco de dados de antivírus) não tenham mudado. As informações de cada arquivo são armazenadas em um banco de dados especial. Essa tecnologia é usada nos modos de proteção em tempo real e de verificação por demanda.

Por exemplo, você tem um arquivo comprimido que foi verificado pelo aplicativo da Kaspersky Lab e ao qual foi atribuído o status não infectado. Na próxima verificação, o aplicativo vai ignorar esse arquivo comprimido, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Se você alterou o conteúdo do arquivo comprimido, adicionando um novo objeto a ele, modificou as configurações de verificação ou atualizou o banco de dados de antivírus, o arquivo comprimido será verificado novamente.

Limitações da tecnologia iChecker:

essa tecnologia não trabalha com arquivos grandes, pois é mais rápido verificar o arquivo que analisar se ele foi modificado desde sua última verificação;

a tecnologia dá suporte a um número limitado de formatos (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

V

VERIFICAÇÃO DO TRÁFEGO

Verificação em tempo real dos objetos transmitidos por todos os protocolos (por exemplo, HTTP, FTP, etc.) que usa informações da versão mais recente do banco de dados.

VÍRUS DE INICIALIZAÇÃO

Um vírus que infecta os setores de inicialização do disco rígido de um computador. O vírus faz o sistema carregá-lo na memória durante a reinicialização e direcionar o controle para o código do vírus em vez do código do carregamento de inicialização original.

VÍRUS DESCONHECIDO

Um novo vírus sobre o qual não há informações nos bancos de dados. Em geral, os vírus desconhecidos são detectados pelo aplicativo em objetos usando o analisador heurístico, e esses objetos são classificados como possivelmente infectados.

KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997. Atualmente, é líder no desenvolvimento de uma grande variedade de produtos de software de segurança de informações de alto desempenho, incluindo sistemas antivírus, antispam e anti-hacking.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa possui escritórios no Reino Unido, França, Alemanha, Japão, Holanda, China, Polônia, Romênia e EUA (Califórnia). Um novo escritório da empresa foi aberto recentemente na França, o Centro Europeu de Pesquisa Antivírus. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas no mundo inteiro.

Atualmente, a Kaspersky Lab emprega mais de mil especialistas altamente qualificados, incluindo 10 detentores de mestrado e 16 detentores de PhD. Todos os especialistas sênior em antivírus da Kaspersky Lab fazem parte da CARO (Computer Anti-Virus Researchers Organization).

Os bens mais valiosos de nossa empresa são o conhecimento exclusivo e a especialização coletiva acumulada nos 14 anos de combate contínuo aos vírus de computador. Uma análise completa das atividades de vírus de computador permite aos especialistas da empresa prever as tendências de desenvolvimento de malware e fornecer aos nossos usuários uma proteção oportuna contra os novos tipos de ataques. Essa vantagem é a base dos produtos e serviços da Kaspersky Lab. Os produtos da empresa estão sempre um passo à frente de outros fornecedores, oferecendo proteção antivírus abrangente aos nossos clientes.

Os anos de muito trabalho tornaram a empresa um dos principais desenvolvedores de software antivírus. A Kaspersky Lab foi a primeira empresa a desenvolver vários dos padrões modernos dos software antivírus. O principal produto da empresa, o Kaspersky Anti-Virus, protege de forma confiável todos os tipos de sistemas de computador contra ataques de vírus, incluindo estações de trabalho, servidores de arquivos, sistemas de email, firewalls, gateways da Internet e computadores portáteis. Suas ferramentas de gerenciamento fáceis de usar maximizam a automação da proteção antivírus de computadores e redes corporativas. Diversos desenvolvedores de todo o mundo usam o kernel do Kaspersky Anti-Virus em seus produtos, incluindo Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab dispõem de vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a conformidade total com seus requisitos empresariais específicos. Nós projetamos, implementamos e damos suporte a sistemas corporativos de antivírus. O banco de dados de antivírus da Kaspersky Lab é atualizado de hora em hora. A empresa fornece aos seus clientes serviço de suporte técnico 24 horas em vários idiomas.

Caso tenha dúvidas, comentários ou sugestões, você pode entrar em contato conosco através de nossos distribuidores ou diretamente com a Kaspersky Lab. Será um prazer ajudá-lo em qualquer assunto relacionado aos nossos produtos, por telefone ou email. Você receberá respostas completas e abrangentes a todas as suas perguntas.

Site oficial da Kaspersky Lab:	http://www.kaspersky.com
Enciclopédia de vírus:	http://www.securelist.com
Laboratório de antivírus:	newvirus@kaspersky.com (somente para o envio de objetos suspeitos em arquivos comprimidos) http://support.kaspersky.com/virlab/helpdesk.html (para o envio de solicitações aos analistas de vírus)
Fórum da Kaspersky Lab na Web:	http://forum.kaspersky.com

INFORMAÇÕES SOBRE CÓDIGO DE TERCEIROS

Foi usado código de terceiros no desenvolvimento do aplicativo.

NESTA SEÇÃO:

Código do programa 185

Ferramentas de desenvolvimento 214

Código do programa distribuído 218

Outras informações 227

CÓDIGO DO PROGRAMA

Foi usado código de terceiros no desenvolvimento do aplicativo.

NESTA SEÇÃO:

AGG 2.4 187

ADOBE ABI-SAFE CONTAINERS 1.0 188

BOOST 1.39.0 188

BZIP2/LIBBZIP2 1.0.5 188

CONVERTUTF 188

CURL 7.19.4 189

DEELX - REGULAR EXPRESSION ENGINE 1.2 189

EXPAT 1.2, 2.0.1 189

FASTSCRIPT 1.90 190

FDLIBM 5.3 190

FLEX: THE FAST LEXICAL ANALYZER 2.5.4 190

FMT.H 190

GDTOA 190

GECKO SDK 1.8, 1.9, 1.9.1 191

ICU4C 4.0.1 199

INFO-ZIP 5.51 199

JSON4LUA 0.9.30 200

LIBGD 2.0.35 200

LIBJPEG 6B 201

LIBM (lrint.c v 1.4, lrintf.c,v 1.5) 202

LIBPNG 1.2.8, 1.2.9, 1.2.42 203

LIBUNGIF 3.0 203

LIBXDR 203

LREXLIB 2.4 204

LUA 5.1.4 204

LZMALIB 4.43 205

MD5.H 205

MD5.H 205

MD5-CC 1.02 205

OPENSSL 0.9.8K 206

PCRE 7.7, 7.9 207

SHA1.C 1.2 209

STLPORT 5.2.1 209

SVCCTL.IDL 209

TINYXML 2.5.3 209

VISUAL STUDIO CRT SOURCE CODE 8.0 209

WINDOWS TEMPLATE LIBRARY 8.0 210

ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3 214

AGG 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Anti-Grain Geometry has dual licensing model. The Modified BSD License was first added in version v2.4 just for convenience. It is a simple, permissive non-copyleft free software license, compatible with the GNU GPL. It's well proven and recognizable. See http://www.fsf.org/licensing/licenses/index_html#ModifiedBSD for details.

Note that the Modified BSD license DOES NOT restrict your rights if you choose the Anti-Grain Geometry Public License.

Anti-Grain Geometry Public License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty, and with no claim as to its suitability for any purpose.

Modified BSD License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ADOBE ABI-SAFE CONTAINERS 1.0

Copyright (C) 2005, Adobe Systems Incorporated

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVEN SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BOOST 1.39.0

Copyright (C) 2008, Beman Dawes

BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007 Julian R Seward.

CONVERTUTF

Copyright (C) 2001-2004, Unicode, Inc

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

CURL 7.19.4

Copyright (C) 1996-2009, Daniel Stenberg

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2009, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

DEELX - REGULAR EXPRESSION ENGINE 1.2

Copyright (C) 2006, RegExLab.com

http://www.regexlab.com/deelx/

EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper

Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, Expat maintainers

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FASTSCRIPT 1.90

Copyright (C) Fast Reports Inc

FDLIBM 5.3

Copyright (C) 2004, Sun Microsystems, Inc

Permission to use, copy, modify, and distribute this software is freely granted, provided that this notice is preserved.

FLEX: THE FAST LEXICAL ANALYZER 2.5.4

Copyright (C) 1990, The Regents of the University of California

---

This code is derived from software contributed to Berkeley by Vern Paxson.

The United States Government has rights in this work pursuant to contract no. DE-AC03-76SF00098 between the United States Department of Energy and the University of California.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

FMT.H

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

GDTOA

Copyright (C) 1998-2002, Lucent Technologies

Copyright (C) 2004, 2005, 2009, David M. Gay

Copyright (C) 1998-2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of Lucent or any of its entities not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

LUCENT DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL LUCENT OR ANY OF ITS ENTITIES BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2004, 2005, 2009 David M. Gay

Permission to use, copy, modify, and distribute this software and its

documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of the author or any of his current or former employers not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR OR ANY OF HIS CURRENT OR FORMER EMPLOYERS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

GECKO SDK 1.8, 1.9, 1.9.1

Copyright (C) Mozilla Foundation

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1,1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1,2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1,3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1,4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1,5. "Executable" means Covered Code in any form other than Source Code.

1,6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1,7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1,8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1,9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1,10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1,11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1,12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2,1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims: under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2,2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale,

have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3,1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3,2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3,3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3,4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3,5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3,6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3,7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6,1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6,2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6,3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8,1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8,2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8,3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8,4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48

C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License

Version 1.1 (the "License"); you may not use this file except in

compliance with the License. You may obtain a copy of the License at

http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS"

basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the

License for the specific language governing rights and limitations

under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. Todos os direitos reservados.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms

of the _____ license (the "[___] License"), in which case the

provisions of [_____] License are applicable instead of those

above. If you wish to allow use of your version of this file only

under the terms of the [____] License and not to allow others to use

your version of this file under the MPL, indicate your decision by

deleting the provisions above and replace them with the notice and

other provisions required by the [___] License. If you do not delete

the provisions above, a recipient may use your version of this file

under either the MPL or the [___] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments,

including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape

Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator

client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape

lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original

Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code.

To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may

choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if

such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public

License Version 1.1 (the "License"); you may not use this file

except in compliance with the License. You may obtain a copy of

the License at http://www.mozilla.org/NPL/

Software distributed under the License is distributed on an "AS

IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or

implied. See the License for the specific language governing

rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released

March 31, 1998.

The Initial Developer of the Original Code is Netscape

Communications Corporation. Portions created by Netscape are

Copyright (C) 1998-1999 Netscape Communications Corporation. All

Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the

terms of the _____ license (the "[___] License"), in which case

the provisions of [_____] License are applicable instead of

those above. If you wish to allow use of your version of this

file only under the terms of the [____] License and not to allow

others to use your version of this file under the NPL, indicate

your decision by deleting the provisions above and replace them

with the notice and other provisions required by the [___]

License. If you do not delete the provisions above, a recipient

may use your version of this file under either the NPL or the

[___] License."

ICU4C 4.0.1

Copyright (C) 1995-2008, International Business Machines Corporation and others

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

JSON4LUA 0.9.30

Copyright (C) 2009, Craig Mason-Jones

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBGD 2.0.35

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant

P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@lucent.com).

Portions copyright 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 Pierre-Alain Joye (pierre@libgd.org).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

LIBJPEG 6B

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

==========

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBM (LRINT.C V 1.4, LRINTF.C,V 1.5)

Copyright (C) 2004, Matthias Drochner

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBPNG 1.2.8, 1.2.9, 1.2.42

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR

Copyright (C) Sun Microsystems, Inc

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

LREXLIB 2.4

Copyright (C) 2000-2008, Reuben Thomas Copyright (C) 2004-2008, Shmuel Zeigerman

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LUA 5.1.4

Copyright (C) 1994-2008, Lua.org, PUC-Rio

Lua License

Lua is licensed under the terms of the MIT license reproduced below.

This means that Lua is free software and can be used for both academic and commercial purposes at absolutely no cost.

For details and rationale, see http://www.lua.org/license.html .

Copyright (C) 1994-2008 Lua.org, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LZMALIB 4.43

MD5.H

Copyright (C) 1999, Aladdin Enterprises

MD5.H

Copyright (C) 1990, RSA Data Security, Inc

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

MD5-CC 1.02

Copyright (C) 1991-1992, RSA Data Security, Inc

Copyright (C) 1995, Mordechai T. Abzug

This software contains a C++/object oriented translation and modification of MD5 (version 1.02) by Mordechai T. Abzug. Translation and modification (c) 1995 by Mordechai T. Abzug

Copyright 1991-1992 RSA Data Security, Inc.

The MD5 algorithm is defined in RFC 1321. This implementation is derived from the reference C code in RFC 1321 which is covered by the following copyright statement:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

OPENSSL 0.9.8K

Copyright (C) 1998-2008, The OpenSSL Project

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project

for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

PCRE 7.7, 7.9

Copyright (C) 1997-2009, University of Cambridge

Copyright (C) 2007-2008, Google Inc

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2009 University of Cambridge

All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2007-2008, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

SHA1.C 1.2

Author Steve Reid (steve@edmweb.com)

STLPORT 5.2.1

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999-2003, Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

SVCCTL.IDL

Copyright (C) 2010, Microsoft Corporation

TINYXML 2.5.3

Copyright (C) 2000-2006, Lee Thomason

VISUAL STUDIO CRT SOURCE CODE 8.0

Copyright (C) Microsoft Corporation

WINDOWS TEMPLATE LIBRARY 8.0

Copyright (C) Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler

FERRAMENTAS DE DESENVOLVIMENTO

Foram usadas ferramentas de desenvolvimentos e outros recursos de terceiros no desenvolvimento do aplicativo.

NESTA SEÇÃO:

MS DDK 4.0, 2000 214

MS WDK 6000, 6001, 6002..... 214

WINDOWS INSTALLER XML (WIX) TOOLSET 3.0 214

MS DDK 4.0, 2000

Copyright (C) Microsoft Corporation

MS WDK 6000, 6001, 6002

Copyright (C) 2001-2007, Microsoft Corporation

WINDOWS INSTALLER XML (WIX) TOOLSET 3.0

Copyright (C) Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE

EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

CÓDIGO DO PROGRAMA DISTRIBUÍDO

O código de programas de terceiros independente é distribuído no aplicativo no formato original ou binário, sem alterações.

NESTA SEÇÃO:

GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE) 219

SYSLINUX 3.86 (FILE SYSLINUX.EXE) 223

GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE)

Copyright (C) 1999, 2000, 2001, 2002, 2004, 2005 Free Software Foundation, Inc

---

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of

preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

SYSLINUX 3.86 (FILE SYSLINUX.EXE)

Copyright (C) 1994-2010, H. Peter Anvin et al

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of

preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.  This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

OUTRAS INFORMAÇÕES

Informações adicionais sobre código de terceiros.

A biblioteca de programas Agava-C, desenvolvida pela OOO "R-Alpha", é usada na verificação de assinaturas digitais.

O Software pode incluir alguns programas licenciados (ou sublicenciados) para o usuário sob a Licença Pública Geral GNU ou outras licenças de software livre similares que, entre outros direitos, permitem que o usuário copie, modifique e redistribua certos programas, ou partes deles, e tenha acesso ao código fonte ("Software de Código Aberto"). Se tais licenças dispuserem que, para qualquer software distribuído a alguém em um formato binário executável, o código fonte também seja oferecido para esses usuários, então ele deve ser disponibilizado diante pedido enviado para source@kaspersky.com ou ser fornecido junto com o Software.

A biblioteca de programas Crypto C, desenvolvida pela OOO "CryptoEx", http://www.cryptoex.ru, é usada na verificação de assinaturas digitais.

ÍNDICE

A

Análise heurística
- Antivírus da Web 105
- Antivírus de Arquivos 94
- Antivírus de Email 99

Antivírus da Web
- análise heurística 105
- banco de dados de endereços da Web de phishing 104
- Consultor de URLs Kaspersky 106
- escopo de proteção 107
- Navegação Segura 106
- nível de segurança 103
- otimização da verificação 106
- resposta a uma ameaça 104

Antivírus de Arquivos
- análise heurística 94
- escopo de proteção 92
- modo de verificação 93
- nível de segurança 93
- otimização da verificação 96
- pausando 91
- resposta a uma ameaça 94
- tecnologia de verificação 94
- verificação de arquivos compostos 95

Antivírus de Email
- análise heurística 99
- escopo de proteção 98
- filtragem de anexos 99
- nível de segurança 98
- resposta a uma ameaça 99
- verificação de arquivos compostos 100

Antivírus de IM
- banco de dados de endereços da Web de phishing 109
- escopo de proteção 109

Atualização
- configurações regionais 87
- fonte de atualização 86
- revertendo a última atualização 89
- servidor proxy 89

Atualizando de uma pasta local 87

Autodefesa do aplicativo 123

B

Banco de dados de endereços de phishing
- Antivírus da Web 104
- Antivírus de IM 109

C

Configuração do Navegador 128

Consultor de URLs Kaspersky
- Antivírus da Web 106

D

Defesa Proativa
- grupo de aplicativos confiáveis 111
- lista de atividades perigosas 111

regra de monitoramento de atividades perigosas 111
Desativando/ativando a proteção em tempo real 53
Desempenho do computador 121
Desinstalação
aplicativo 37
Disco de Recuperação 66

E

Escopo de proteção
Antivírus da Web 107
Antivírus de Arquivos 92
Antivírus de Email 98
Antivírus de IM 109

I

Ícone da área de notificação da barra de tarefas 42

J

Janela principal do aplicativo 44

L

Licença
ativando o aplicativo 55
Contrato de Licença do Usuário Final 39

M

Menu de contexto 43

N

Nível de segurança
Antivírus da Web 103
Antivírus de Arquivos 93
Antivírus de Email 98
Notificações 57
desativando 137
desativando o sinal sonoro 137
entrega de notificações por email 137
tipos de notificações 137

P

Pasta de instalação 30
Programação
atualização 88
verificação de vírus 80

Q

Quarentena e Backup 124

R

Rastreamento
carregando resultados de rastreamento 145
criando um arquivo de rastreamento 145
Reação à ameaça
verificação de vírus 82
Rede
conexões criptografadas 114
portas monitoradas 117

Relatórios
exibir 69
filtragem 132
pesquisa de eventos 132
salvando em arquivo 133
selecionando um componente ou uma tarefa 131
Renovação da licença 56
Requisitos de software 26
Resposta a uma ameaça
Antivírus da Web 104
Antivírus de Arquivos 94
Antivírus de Email 99
Restaurando as configurações padrão 69
Restringindo o acesso ao aplicativo 76

T

Teclado Virtual 62

V

Verificação
ação com objetos detectados 82
conta 82
execução automática de tarefas ignoradas 80
iniciando a tarefa 58
nível de segurança 79
otimização da verificação 84
programação 80
tecnologias de verificação 81
tipos de objetos a serem verificados 82
verificação de arquivos compostos 83
verificação de vulnerabilidades 85

Z

Zona confiável
aplicativos confiáveis 119
regras de exclusão 119